EXHIBIT 1

US007633385B2

(12) **United States Patent**
Cohn et al.

(10) **Patent No.:** **US 7,633,385 B2**
(45) **Date of Patent:** **Dec. 15, 2009**

(54) **METHOD AND SYSTEM FOR COMMUNICATING WITH AND CONTROLLING AN ALARM SYSTEM FROM A REMOTE SERVER**

(75) Inventors: **Alan Wade Cohn**, Austin, TX (US); **Ronald E. Battles**, Cedar Park, TX (US); **David Proft**, Austin, TX (US); **Scott William Shumate**, Austin, TX (US)

(73) Assignee: **uControl, Inc.**, Austin, TX (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 345 days.

(21) Appl. No.: **11/711,972**

(22) Filed: **Feb. 28, 2007**

(65) **Prior Publication Data**

US 2008/0204190 A1 Aug. 28, 2008

(51) **Int. Cl.**
G08B 29/00 (2006.01)
G08B 9/00 (2006.01)

(52) **U.S. Cl.** **340/506**; 340/286.02

(58) **Field of Classification Search** 340/506–513, 340/541–567, 691.1–691.6, 693.5–693.12, 340/3.2–3.32, 3.7, 3.9, 825.36–7.61, 286.01, 340/286.02, 815.48, 815.49
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,134,644	A	7/1992	Garton et al.	379/39
5,438,607	A	8/1995	Przygoda, Jr. et al.	379/38
5,499,014	A	3/1996	Greenwaldt	340/539
5,717,379	A	2/1998	Peters	340/539
5,777,551	A	7/1998	Hess	340/541
5,892,442	A	4/1999	Ozery	340/539
5,943,394	A	8/1999	Ader et al.	379/40
6,032,036	A	2/2000	Maystre et al.	455/404
6,038,289	A	3/2000	Sands	379/26
6,049,272	A	4/2000	Lee et al.	340/539
6,049,273	A	4/2000	Hess	340/539
6,052,052	A	4/2000	Delmonaco	340/539
6,067,346	A	5/2000	Akhteruzzaman et al.	379/39
6,661,340	B1	12/2003	Saylor et al.	340/517

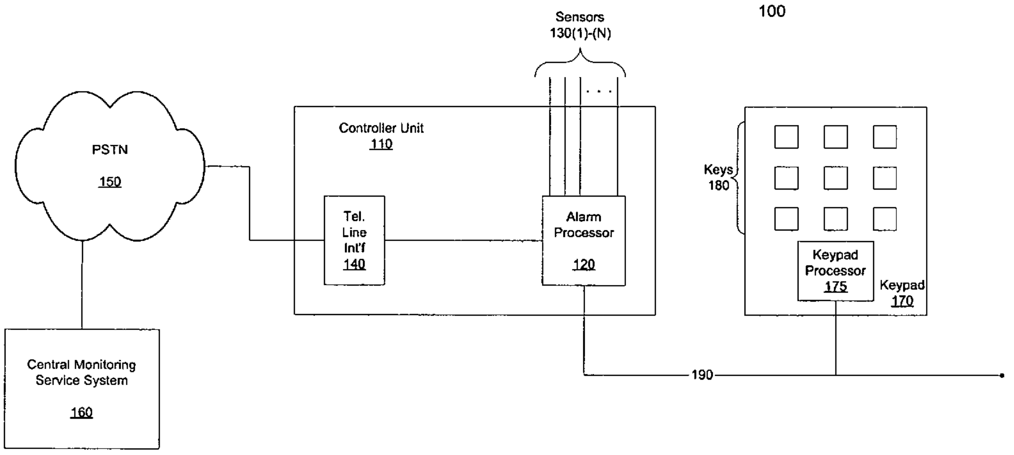
(Continued)

Primary Examiner—Jennifer Mehmood
(74) *Attorney, Agent, or Firm*—Campbell Stephenson LLP; Jonathan N. Geld

(57) **ABSTRACT**

A communication system is provided that can be added to a legacy alarm system to provide a plurality of communication modes to a remote server system from the legacy alarm system and provide remote control and monitoring to a user of the system via two-way communication links. The communication system can be configured to communicate with an alarm processor of the legacy alarm system through use of a keypad bus typically used by the legacy alarm system for communication between the alarm processor and one or more keypads. Communication modes that can be provided by embodiments of the present invention can include, for example, communication over a public switched telephone network, cellular transmission, broadband transmission, and the like. The communication system can monitor all configured communication modes and determine which communication mode is the best for providing communication between the alarm system and the remote server. Through these communication modes and by virtue of being coupled to the alarm processor via the keypad bus, the communication system can provide both transmission to the remote server of the status and alarm condition of the legacy alarm system as well as provide control signals from the remote server to the legacy alarm system. The remote server provides pre-determined responses to information received from the alarm system, including providing alarm system condition information to a user or a monitoring station for response.

16 Claims, 8 Drawing Sheets



U.S. PATENT DOCUMENTS

6,956,477 B2 * 10/2005 Chun 340/541
7,053,764 B2 * 5/2006 Stilp 340/506
7,248,161 B2 * 7/2007 Spoltore et al. 340/539.14
2007/0226182 A1 * 9/2007 Sobotka et al. 707/3

* cited by examiner

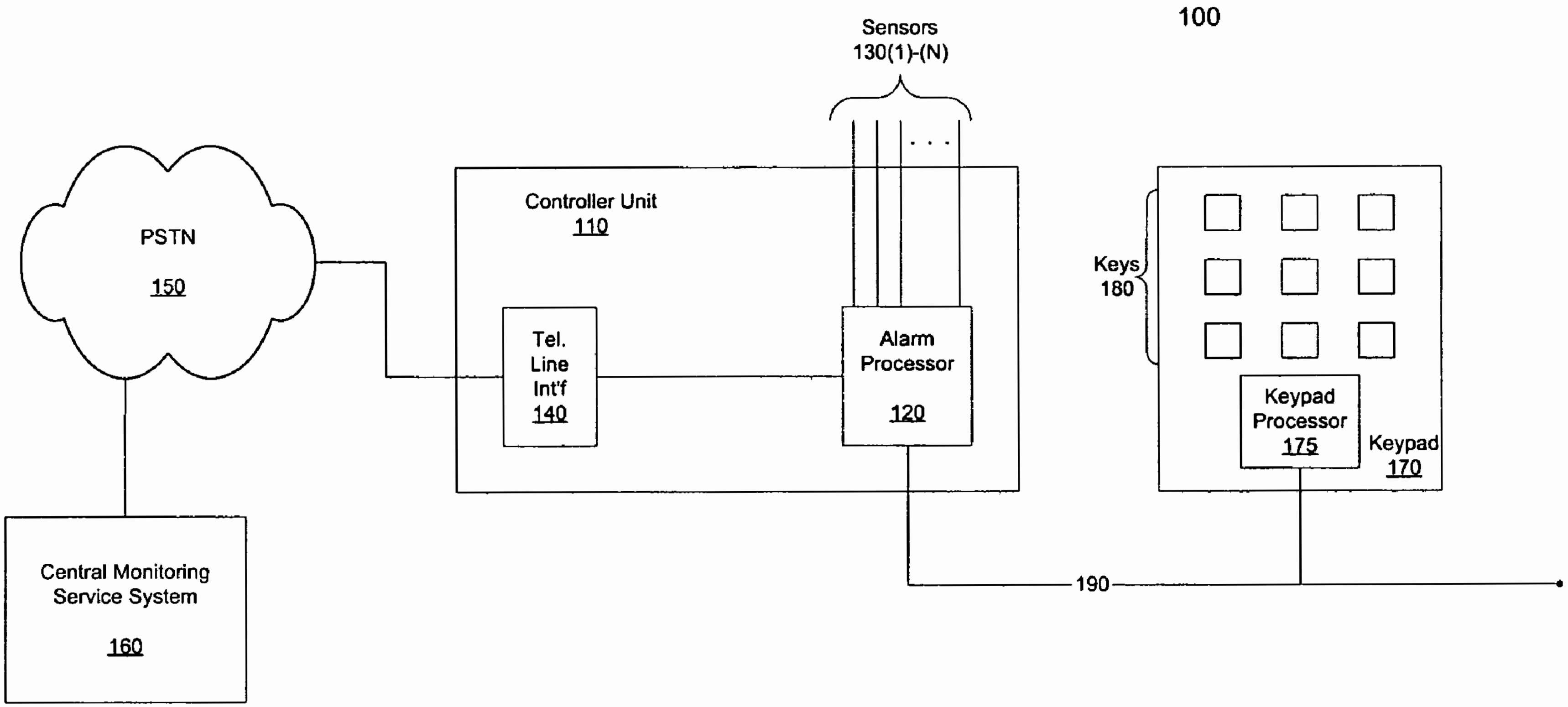

100
Sensors
130(1)-(N)
PSTN
150
Controller Unit
110
Tel.
Line
Int'f
140
Alarm
Processor
120
Keys
180
Keypad
Processor
175
Keypad
170
190
Central Monitoring
Service System
160

Figure 1

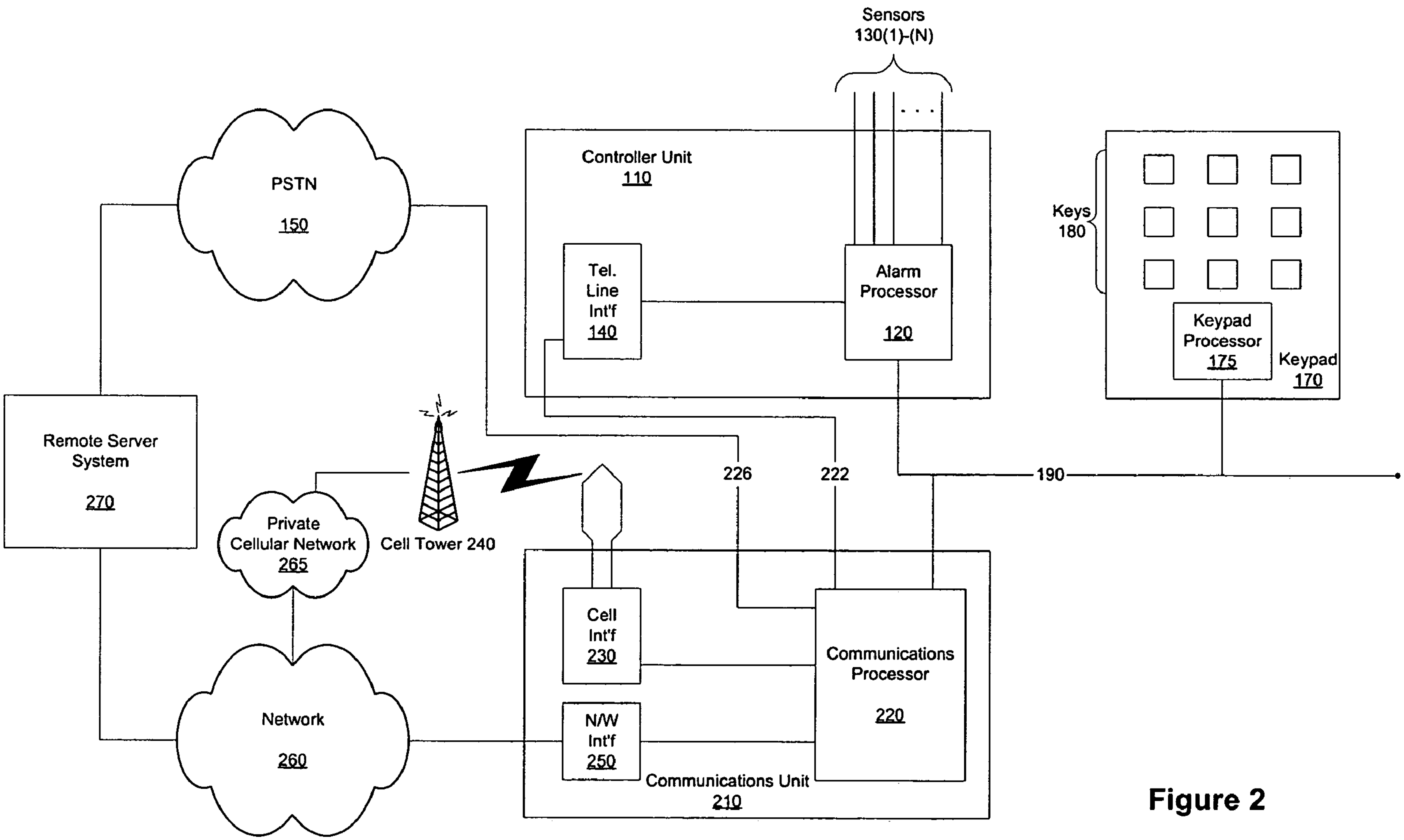

Sensors
130(1)-(N)
Controller Unit
110
Tel.
Line
Int'f
140
Alarm
Processor
120
Keys
180
Keypad
Processor
175
Keypad
170
PSTN
150
Remote Server
System
270
Private
Cellular Network
265
Cell Tower 240
226
222
190
Cell
Int'f
230
Communications
Processor
220
N/W
Int'f
250
Communications Unit
210
Network
260

Figure 2

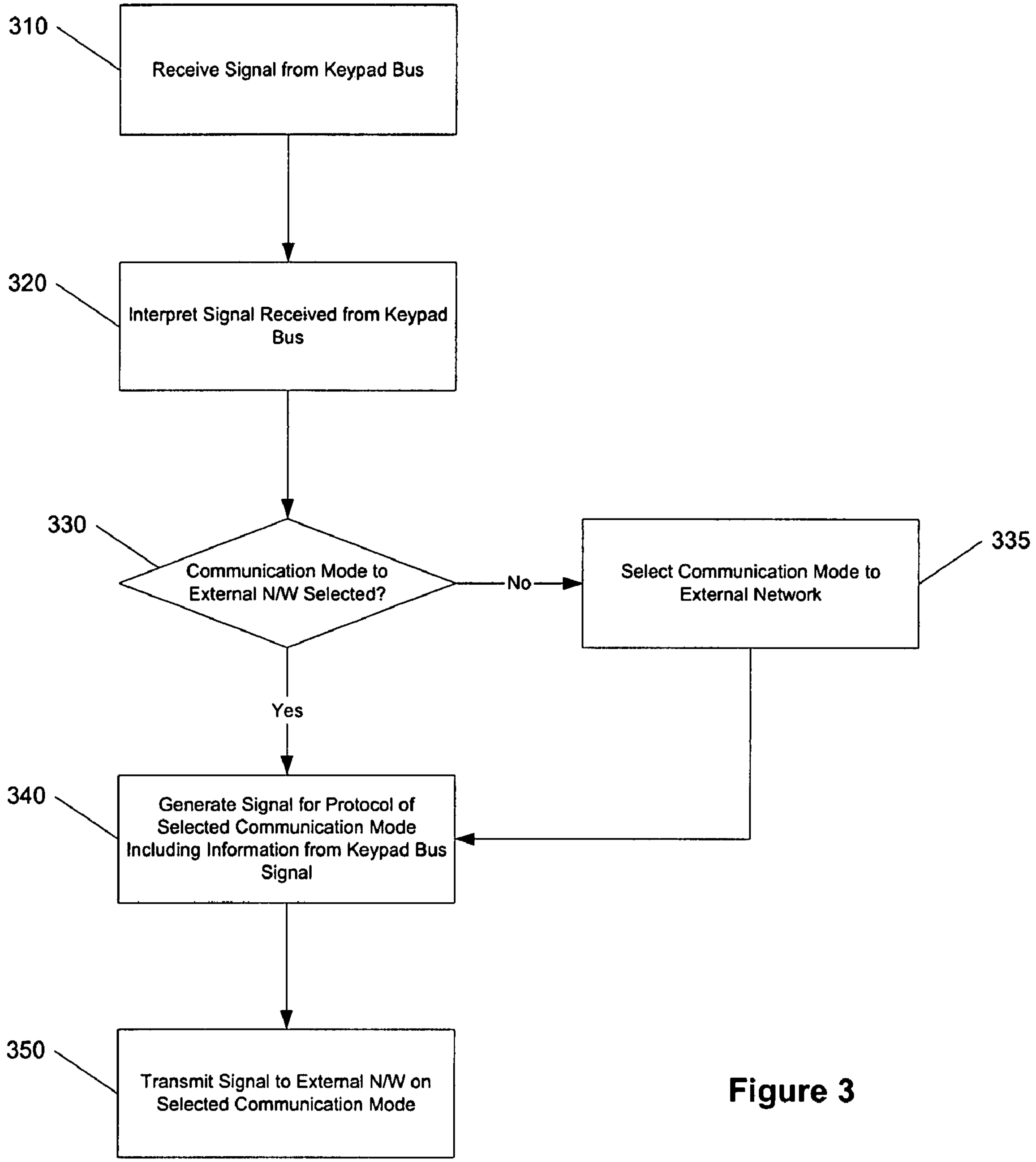

310
Receive Signal from Keypad Bus
320
Interpret Signal Received from Keypad Bus
330
Communication Mode to External N/W Selected?
No
335
Select Communication Mode to External Network
Yes
340
Generate Signal for Protocol of Selected Communication Mode Including Information from Keypad Bus Signal
350
Transmit Signal to External N/W on Selected Communication Mode

Figure 3

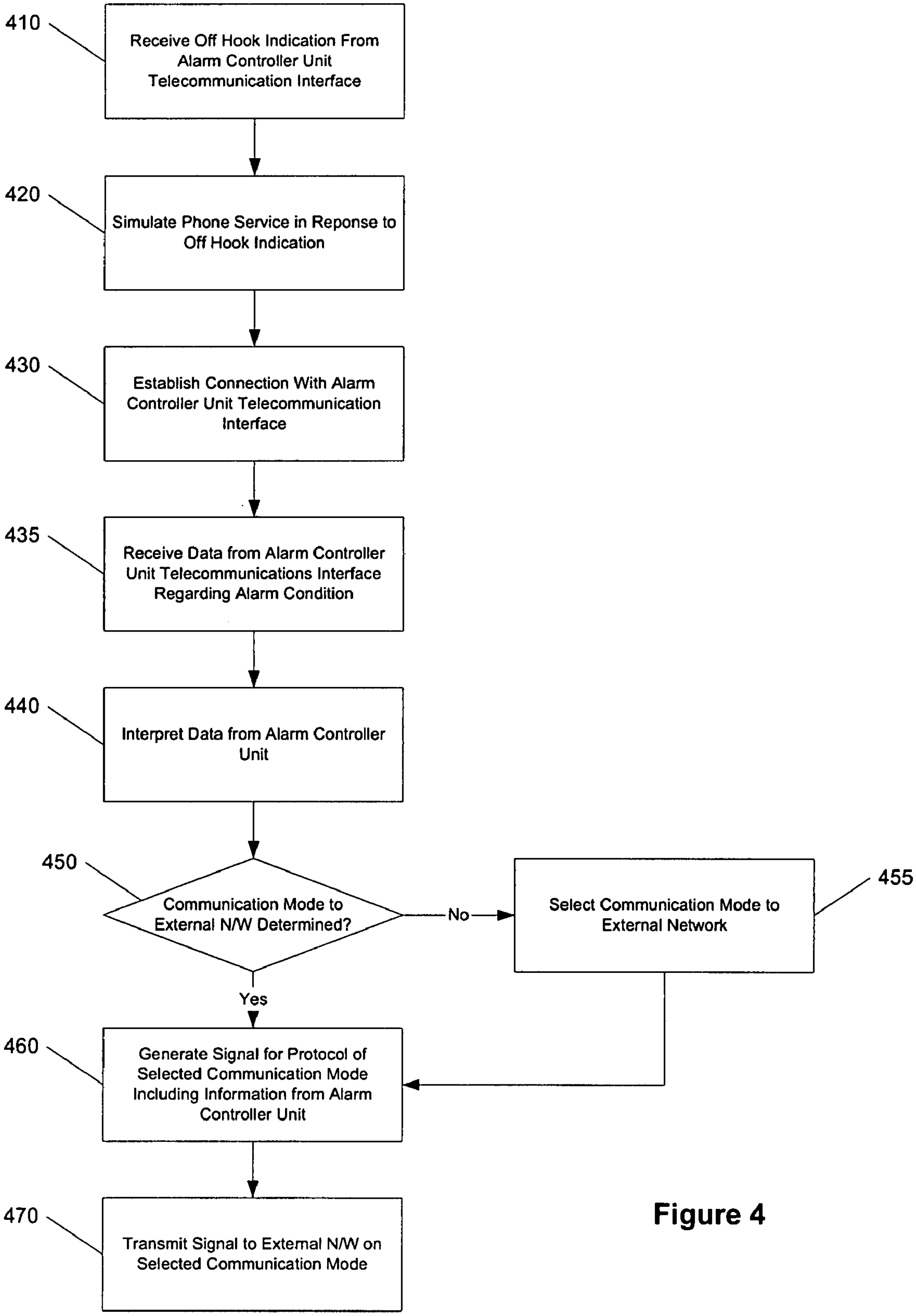

410
Receive Off Hook Indication From Alarm Controller Unit Telecommunication Interface
420
Simulate Phone Service in Reponse to Off Hook Indication
430
Establish Connection With Alarm Controller Unit Telecommunication Interface
435
Receive Data from Alarm Controller Unit Telecommunications Interface Regarding Alarm Condition
440
Interpret Data from Alarm Controller Unit
450
Communication Mode to External N/W Determined?
No
Yes
455
Select Communication Mode to External Network
460
Generate Signal for Protocol of Selected Communication Mode Including Information from Alarm Controller Unit
470
Transmit Signal to External N/W on Selected Communication Mode

Figure 4

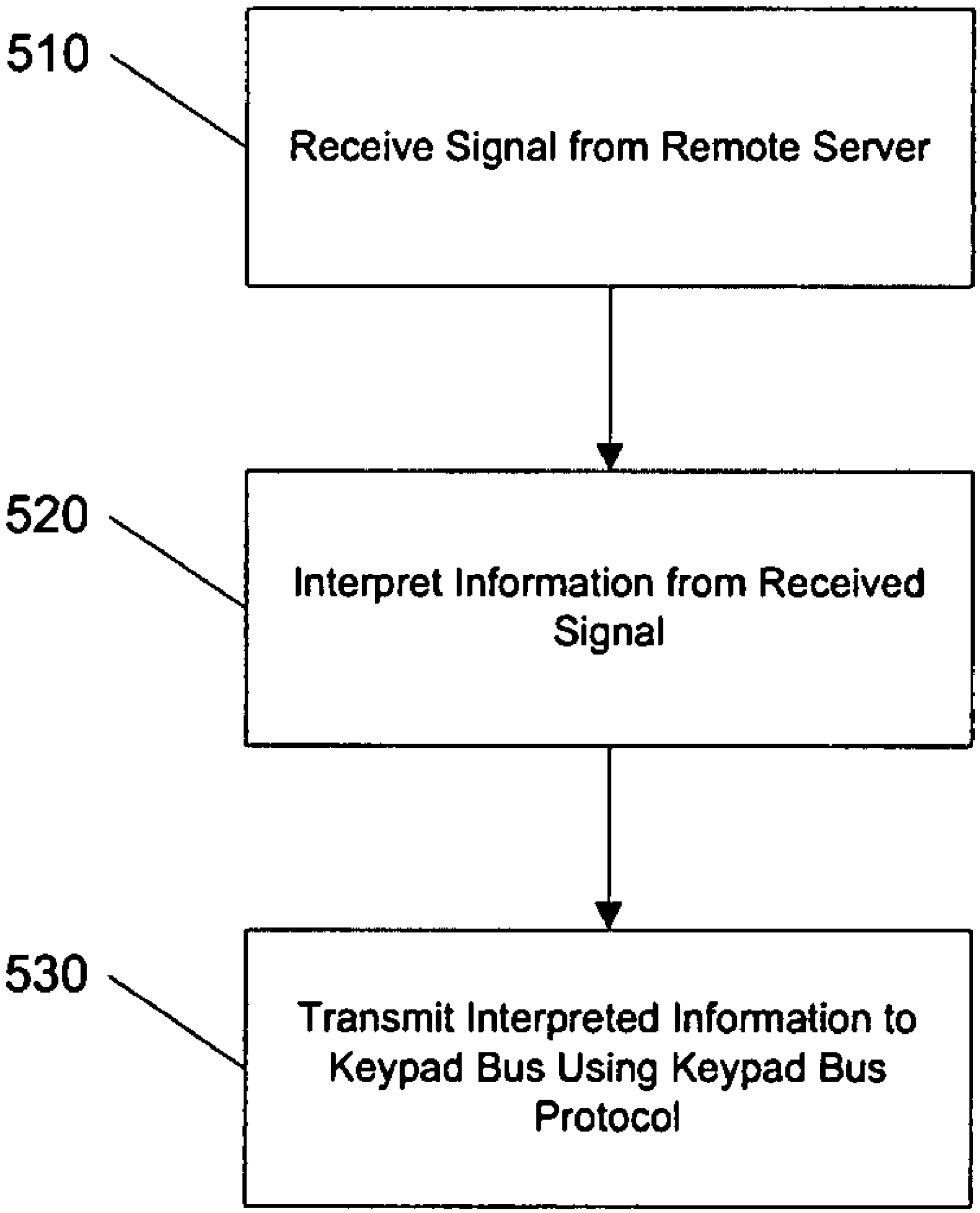

510
Receive Signal from Remote Server
520
Interpret Information from Received Signal
530
Transmit Interpreted Information to Keypad Bus Using Keypad Bus Protocol

Figure 5

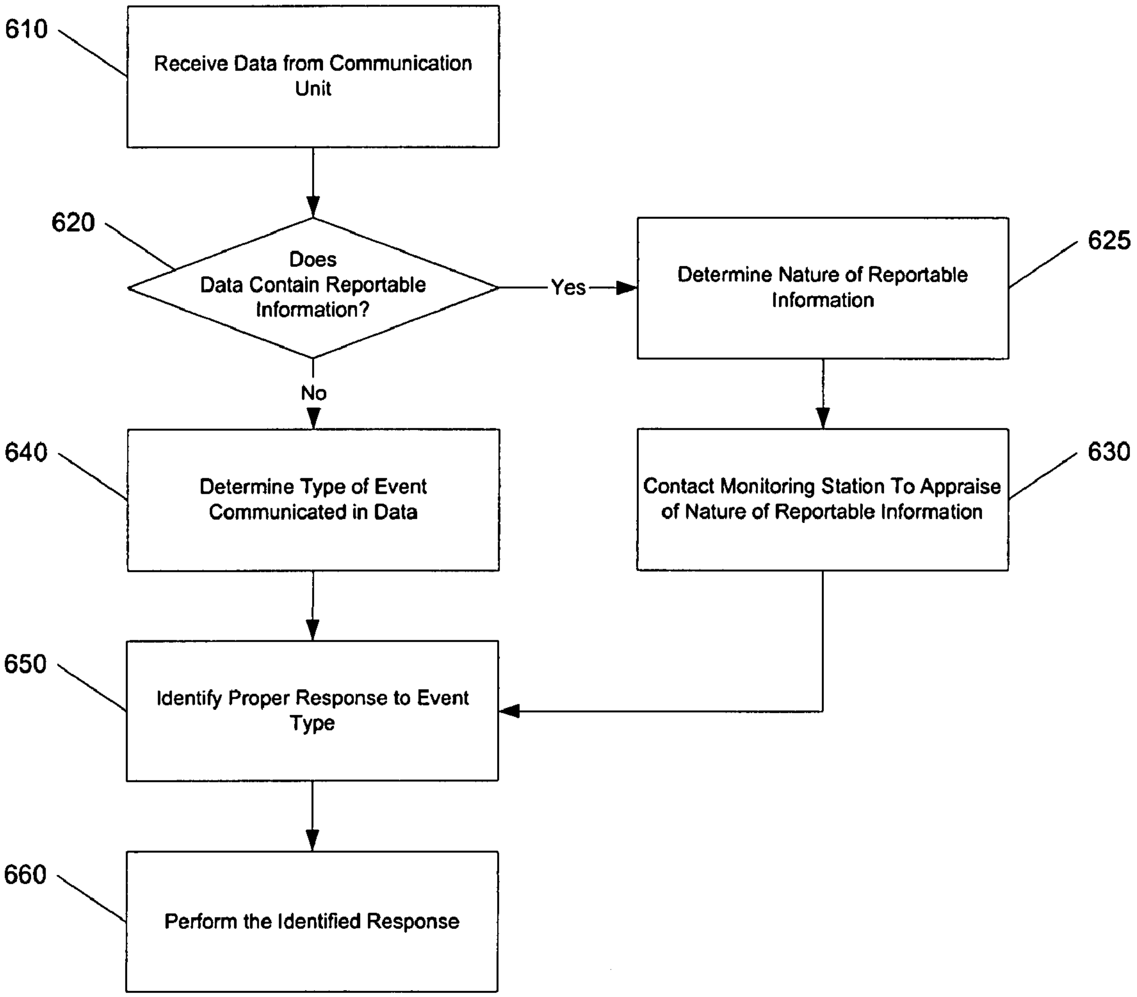

610
Receive Data from Communication Unit
620
Does Data Contain Reportable Information?
Yes
No
625
Determine Nature of Reportable Information
630
Contact Monitoring Station To Appraise of Nature of Reportable Information
640
Determine Type of Event Communicated in Data
650
Identify Proper Response to Event Type
660
Perform the Identified Response

Figure 6

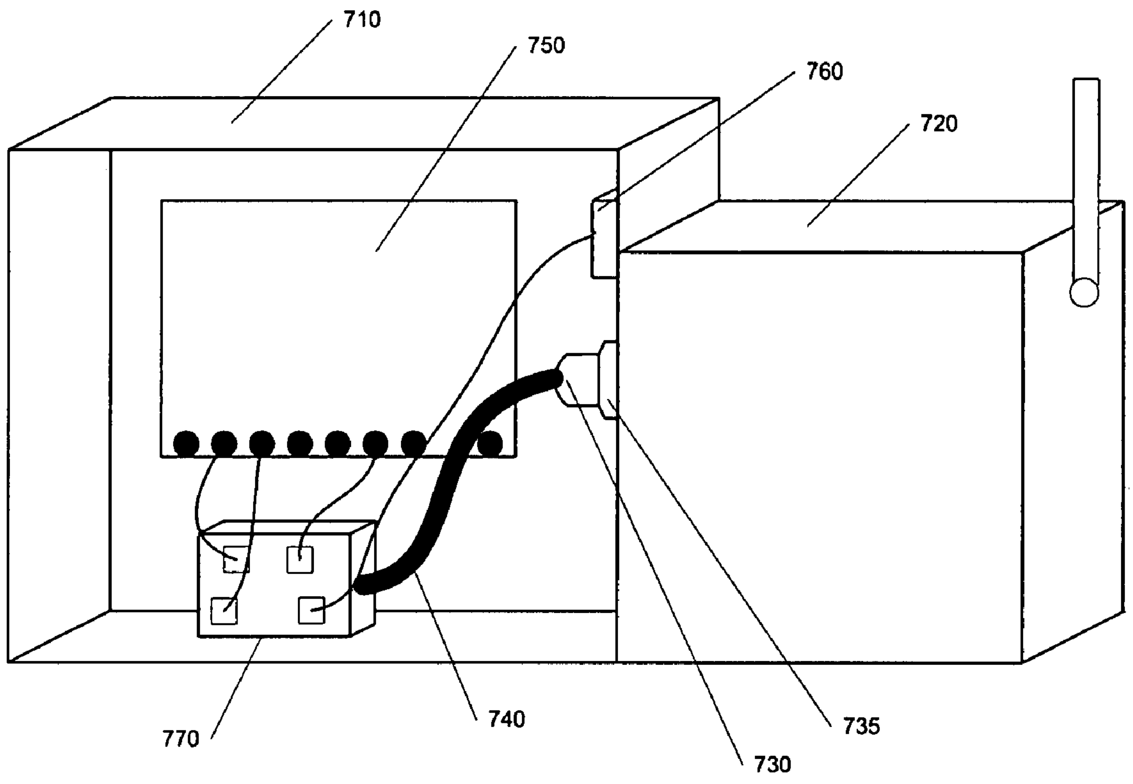

710
750
760
720
770
740
730
735

Figure 7

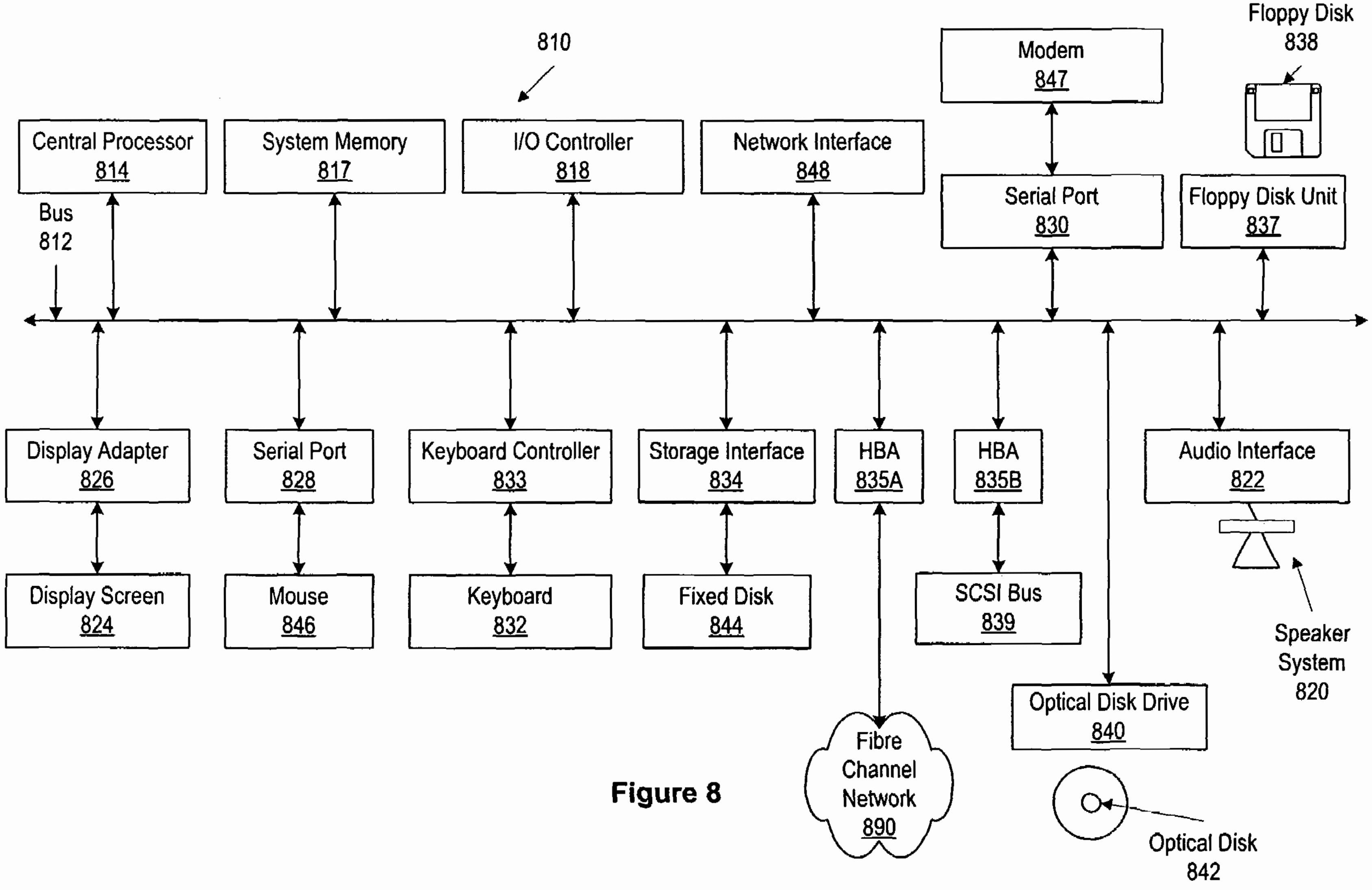

810
Central Processor
814
System Memory
817
I/O Controller
818
Network Interface
848
Modem
847
Serial Port
830
Floppy Disk
838
Floppy Disk Unit
837
Bus
812
Display Adapter
826
Serial Port
828
Keyboard Controller
833
Storage Interface
834
HBA
835A
HBA
835B
Audio Interface
822
Display Screen
824
Mouse
846
Keyboard
832
Fixed Disk
844
SCSI Bus
839
Speaker
System
820
Optical Disk Drive
840
Fibre
Channel
Network
890
Optical Disk
842

Figure 8

METHOD AND SYSTEM FOR COMMUNICATING WITH AND CONTROLLING AN ALARM SYSTEM FROM A REMOTE SERVER

FIELD OF THE INVENTION

The present invention relates to the field of security systems, and more particularly relates to coupling a legacy alarm system to a server coupled to an external network via a plurality of monitored communication modes, enabling the server to provide control information to the legacy alarm system, and the legacy alarm system to report status and alarm conditions to the server.

BACKGROUND OF THE INVENTION

Security systems alert occupants of a dwelling and emergency authorities of a violation of premises secured by the security system. A typical security system includes a controller connected by wireless or wired connections to sensors deployed at various locations throughout the secured dwelling. In a home, sensors are usually deployed in doorways, windows, and other points of entry. Motion sensors can also be placed strategically within the home to detect unauthorized movement, while smoke and heat sensors can detect the presence of fire.

Security systems are usually connected to a central monitoring service system via a telecommunications line coupled to a public switched telephone network (PSTN). The central monitoring service system can be maintained by a security service provider and continuously monitors all activated subscriber security systems for alarms. Sensor activity occurs when a sensor detects, for example, an opening of a door or window, or presence of movement, or a fire. Sensor activity causes the sensor to send a signal to the controller of the security system. Responsive to receiving the signal, the controller can determine whether the signal represents an alarm condition and, if so, issue an audible alarm to alert the occupants of the dwelling and can originate a data transmission to the central monitoring service system via the telecommunications line. Upon receiving notification of an alarm, the central monitoring service system can determine the type of activity, attempt to contact the dwelling occupants, and alert appropriate authorities of an emergency situation.

Typically, the telecommunications line interconnecting the security system to the central monitoring service system is the dwelling occupant's telephone line. This line usually emanates from and is accessible from the exterior of the dwelling. It is this telecommunications line which delivers a security breach signal to the central monitoring service system via a PSTN.

One drawback of such a security system is that the telecommunications line becomes a potential single point of failure for providing a security breach signal to the central monitoring service system. Should the telephone line be rendered inoperative, for example, by an intruder cutting the telecommunications line prior to attempting entry, or due to other types of telecommunications systems failure, then the security breach signal will fail to be provided to the central monitoring service system and further action, such as notification of the authorities will not occur. Such links between a security system and a central monitoring service system are typically one-way, providing only data from the security system to the central monitoring system, which is another drawback. Such a one-way communication link does not allow for remote access of the security system to monitor or control the system.

Other security systems exist that can provide either a redundant communication mode or two-way communication between the security system and a remote server, either accessed by a central monitoring service system or a user. The drawbacks with regard to these prior art systems are that should a dwelling already have a security system such as that described above, the legacy security system would have to be deinstalled and then replaced by a security system providing redundant communication modes and/or two-way communication. There is no capacity to add such functionality to an existing alarm system. Such replacement of a legacy security system entails high costs, as the controller unit of the legacy security system must be replaced, and the sensors need to be rewired to a new controller unit.

It is therefore desirable to provide a cost-effective solution for enabling legacy (pre-installed) security systems to be remotely controlled and monitored by either a user of the system (e.g., a home owner) or a central monitoring service system, through a plurality of continuously-monitored communication modes.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention may be better understood, and its numerous objects, features and advantages made apparent to those skilled in the art by referencing the accompanying drawings.

FIG. **1** is a simplified block diagram illustrating elements of an alarm system usable with embodiments of the present invention.

FIG. **2** is a simplified block diagram of components of a legacy alarm system coupled to a communications system, in accord with embodiments of the present invention.

FIG. **3** is a simplified flow diagram illustrating steps performed in providing a signal received from a keypad bus to an external network over a selected communication mode, in accord with embodiments of the present invention.

FIG. **4** is a simplified flow diagram illustrating steps for providing information in an alarm signal received from alarm processor's telephone interface to an external network, in accord with embodiments of the present invention.

FIG. **5** is a simplified flow diagram illustrating steps performed in providing control information generated by a remote server to a legacy alarm system, in accord with embodiments of the present invention.

FIG. **6** is a simplified flow diagram illustrating a method performed by a remote server system in response to receiving data from a communications unit, in accord with embodiments of the present invention.

FIG. **7** is a simplified block diagram illustrating one example of a connection between a communication unit and a legacy alarm system controller, in accord with embodiments of the present invention.

FIG. **8** depicts a block diagram of a computer system suitable for implementing embodiments of the present invention.

DETAILED DESCRIPTION

Embodiments of the present invention provide a communication system that can be added to a legacy alarm system to provide a plurality of communication modes to a remote server system from the legacy alarm system and provide remote control and monitoring to a user of the system via two-way communication links. Embodiments of the present invention can be configured to communicate with an alarm processor of the alarm system through use of a keypad bus typically used by the legacy alarm system for communications between the alarm processor and one or more keypads. Communication modes to the remote server system that can be provided by embodiments of the present invention can include, for example, communication over a public switched telephone network, cellular transmission, broadband transmission, and the like. Embodiments of the present invention can monitor all configured communication modes and determine which communication mode is the best for providing communication between the alarm system and the remote server. Through these communication modes and by virtue of being coupled to the alarm processor via the keypad bus, embodiments of the present invention can provide both transmission to the remote server of the status and alarm condition of the legacy alarm system as well as provide control signals from the remote server to the legacy alarm system.

FIG. **1** is a simplified block diagram illustrating elements of a legacy alarm system **100**. Alarm system **100** includes a controller unit **110**. Controller unit **110** includes an alarm processor **120**, which is coupled to sensors **130**(**1**)-(N). Sensors **130**(**1**)-(N) can be installed at various points of entry for a building to detect when such a point of entry is reached, and can also include, for example, motion, smoke, and fire detectors. Alarm processor **120** can define zones each of which can include one or more alarm sensors **130**(**1**)-(N). Alarm processor **120** is further coupled to a telephone line interface **140**. In the event of a triggering of one of sensors **130**(**1**)-(N), alarm processor **120** can instruct telephone line interface **140** to dial a call through public switched telephone network (PSTN) **150** to a central monitoring service system **160**. Alarm processor **120** can then send data through the connection to the central monitoring service system, providing information related to the type of security breach (e.g., identification of zone, fire or intrusion alarm, etc.).

Alarm processor **120** is also coupled to a keypad **170**. Keypad **170** allows a user in the building to control the alarm system by performing tasks such as arming and disarming the alarm system, activating an alarm sequence to activate an audible alarm and call to the central monitoring service system, sending a silent distress signal to the central monitoring service system, and programming and configuring alarm system **100**. Keypad **170** includes a keypad processor **175**, which is coupled to keys **180** through which the user can enter commands. Keypad **170** can also include, for example, visual indicators of the status of the alarm system such as LEDs or a display, which are coupled to the keypad processor. Alarm processor **120** is coupled to keypad processor **175** through a keypad bus **190**. Keypad bus **190** provides communication between the alarm processor and keypad processor using, for example, a serial digital protocol transmitted and received by the processors. One or more keypads can be connected to the alarm processor via the keypad bus.

Through the use of the keypad bus serial digital protocol, the alarm processor can provide to the keypad information such as whether the alarm is armed or disarmed, and whether zones are tripped or not. The keypad processor can provide arming codes and other control information to the alarm processor.

FIG. **2** is a simplified block diagram of components of a legacy alarm system coupled to a communications system in accord with embodiments of the present invention. As discussed above, alarm controller **110** includes a microprocessor **120** that is coupled to sensors **130**(**1**)-(N). Alarm processor **120** is coupled via keypad bus **190** to keypad processor **175** within keypad **170**. Communications unit **210** provides a communications processor **220** that is coupled to alarm processor **120** and keypad processor **175** via keypad bus **190**. Thus, communications processor **220** can exchange data with alarm processor **120** using the serial digital protocol of keypad bus **190**. Communications processor **220** can be configured to automatically determine the type of serial digital protocol being used in communications between alarm processor **120** and keypad processor **175** as part of an initial configuration of communications unit **210** upon being coupled to the keypad bus.

Communications processor **220** is also coupled to controller unit **110** via telecommunications link **222**, which is coupled to the outgoing port of telephone line interface **140**. Communications processor **220** is further coupled to PSTN **150** by telecommunications link **226**, thereby breaking the direct link between telephone line interface **140** and PSTN **150** illustrated in FIG. **1**. Communications processor **220** then serves as an intermediary between alarm unit **110** and PSTN **150**. It is through this link that communications processor **220** can provide communication from alarm controller unit **110** to a remote server system **270** via the PSTN, should that be a selected communication mode (as described below).

Remote server system **270** can be a network-coupled computer system that provides, in part, responsive communication to information received from communications unit **210**. Such responsive communication can be provided to, for example, the user of the alarm system (e.g., a homeowner) or to emergency responders to alarm conditions. Remote server system **270** can also provide communication to communications unit **210**, including, for example, configuration information and updates.

Communications processor **220** can also be coupled to a cellular interface **230** that can provide cellular transmission to a cell tower **240** that is also coupled, directly or indirectly, to a private cellular network **265**, which is further coupled to a network **260**. Through this link, communications processor **220** can provide a cellular transmission communication mode to server system **270**, which is also coupled to network **260**.

Communications processor **220** can also be coupled to a network interface **250**. Network interface **250** can provide a broadband connection to network **260** (e.g., the Internet), which is also coupled to server system **270**. Through network interface **250**, communications processor **220** can provide a broadband communications mode to server system **270**.

In alternate embodiments of communications unit **210**, communications processor **220** can be coupled to other communication interfaces that can provide wireless broadband, Wi-Fi communication, and the like.

The multiple communication modes provided by communication unit **210** avoid the single point of failure (e.g., an external telephone line) present in legacy alarm systems. To this end, it is preferable that multiple communication modes not be transmitted over a common link from a building in which an alarm system is installed.

Communications processor **220** can monitor all of the available communication modes to determine which communication mode is the best for transmitting data to and from server system **270** at any point in time. For example, the communications processor, through network interface **250**, can monitor whether there is an active connection to network **260**. Such monitoring can be performed by, for example, by periodically establishing, or attempting to establish, a connection with server system **270** and monitoring a heartbeat signal. Alternatively, the communications processor can determine availability and viability of a network connection to the server system using, for example, network echo packets (e.g., pinging). Similarly, through cellular interface **230**, communications processor **220** can periodically establish, or attempt to establish, a connection with server system **270** through private cellular network **265** and network **260**. With regard to connections via PSTN **150**, the communications processor can, for example, determine whether there is an appropriate voltage over the telecommunications link **226** from the PSTN. In an event of a voltage drop on telecommunications link **226**, the communications processor can interpret such a drop as an event that needs to be communicated to the remote server (over either the broadband or cellular connection).

As the communications processor determines the best communication mode, that mode is then used for communication between communication unit **210** and server system **270** until a determination is made that an alternate communication mode is more appropriate. Alternatively, the communications processor can be configured to give primary preference to a particular communications mode (e.g., broadband), and then secondary preference to a different communications mode (e.g., cellular), and so on. In such a case, the communications processor will use the primary communications mode unless that communications mode is unavailable and then switch to a secondary (or lower) communications mode, depending upon availability of that mode.

An example communication mode configuration for the controller unit can provide for broadband being the primary communication mode, since broadband connections can be relatively inexpensive to maintain a constant link through and data rates are relatively high. The secondary communication mode can be a cellular connection because of difficulty involved in severing such a connection. But data rates may be lower for the cellular connection, as well as relatively more expensive. Thus, the communication unit can be configured, for example through control settings provided by server **270**, to only communicate a subset of events through cellular connections. To compensate for this reduced event data bandwidth, the communications unit can cache event information, along with time stamps, in a memory local to the communications unit and provide all those events to the server when the broadband connection is restored. Further, PSTN communication can be configured as a tertiary communication mode. Data rates through PSTN can determine a different subset of events reportable through PSTN, and again the communication unit can be configured with that subset. For example, data rates over PSTN can limit the communication unit to only transmit alarm event information over that communication mode. Alternatively, PSTN communication can result in some or all non-alarm, reportable events being cached for later transmission through the PSTN. Further, PSTN communication may limit communication unit-to-server communication to a one-way link, rather than two-way communication provided by broadband and cellular.

As stated above, communications processor **220** and alarm unit **110** are coupled over telecommunications link **222** in order for the communications processor to function as an intermediary between the alarm unit and PSTN **150**. In a legacy system, when alarm processor **120** detects an alarm situation, alarm processor **120** instructs telephone line interface **140** to dial out over PSTN **150** to communicate with the central monitoring service system. Communications processor **220** can simulate the phone service and the central monitoring system and interpret the alarm signals provided by alarm processor **120**. Alarm processor **120** provides such communication using, for example, a ContactID format. Communications processor **220** can read the data supplied by alarm processor **120** over the telecommunications link, interpret that data, and transmit an appropriate signal over the chosen communication mode to server system **270**.

Communications processor **220** can also interpret signals provided by alarm processor **120** over keypad bus **190**, and provide that information to server system **270** over the chosen communication mode. As stated above, such information can include arm/disarm indicators, zone trip information, system trouble (e.g., low battery, clock reset, no power), and the like.

As stated above, communications processor **220** interprets event signals received from alarm processor **120** over either keypad bus **190** or telephone line interface **140**. Communications processor **220** will then generate a signal to send over the selected communication mode to server system **270**. This signal corresponds to the interpretation of the event signal received from the alarm processor. In the case of alarm events received over the telephone line interface, the communications processor can also encapsulate original data received for transmission to the server system. In this manner, should the server system need to further analyze the alarm indication in order to determine a proper response, that data is provided in its original form.

Communications processor **220** can also receive information provided by server system **270** over a communication mode selected by the server system. Communications processor **220** can interpret that received information and format the information for the appropriate serial digital protocol of keypad bus **190**. Communications processor **220** can then provide the information to alarm processor **120** over keypad bus **190**. Through such communication, communications processor **220** emulates keypad communication to alarm processor **120**. Thus, there is no need to reprogram the legacy alarm system to allow the legacy alarm system to be controlled through communication unit **210**.

FIG. **3** is a simplified flow diagram illustrating steps performed in providing a signal received from a keypad bus to an external network over a communication mode, in accord with embodiments of the present invention. A data signal is received from a connection to a keypad bus (**310**), for example, by a communications processor **220**. Prior to receiving the signal, and typically upon initial startup of the communications unit when connected to the keypad bus, an identification of the serial digital protocol of the keypad bus is made. Such a determination of the keypad bus protocol can be made by one of several methods including, for example, analyzing the received data signal from the keypad bus and comparing that signal to expected signal formats for keypad bus protocols, or transmitting a test command from one of a plurality of possible keypad bus protocols and analyzing a received responsive signal for conformity with the protocol of the transmitted signal, or analyzing signals transmitted by a keypad **170** in response to a predetermined code entered into keys **180**, or analyzing timing parameters of the serial digital signal to determine the protocol type.

Using the determined keypad bus protocol, the signal received from the keypad bus can be interpreted (**320**). This interpretation can include determining the nature of the keypad bus signal (e.g., arm/disarm, zone tripped/not tripped, alarm controller status). A determination can then be made as to whether a communication mode to an external network has been previously selected (**330**). If not, then a selection of a communication mode to the external network can be made (**335**). As discussed above, the selection of a communication mode is made in response to periodic or continuous monitoring of the communication modes available to the communications unit. When a communication mode has been selected, a signal can then be generated corresponding to the protocol of the selected communication mode, wherein that signal includes information corresponding to the signal received from the keypad bus (**340**). That generated signal can then be transmitted to the external network via the selected communication mode (**350**). In order to perform such a transmission, it may be necessary to establish a link with the external network and ultimately to a remote server system coupled to the external network (e.g., **270**) in order to effect the data transfer.

FIG. **4** is a simplified flow diagram illustrating steps for providing information in an alarm signal received from alarm processor's telephone interface to an external network, in accord with embodiments of the present invention. As discussed above, upon detecting an alarm condition, such as a sensor breach, an alarm processor of a legacy alarm system will use a phone line to contact a central monitoring service system. Embodiments of the present invention are coupled to the telephone interface of the legacy alarm system and will receive an off hook indication generated by the alarm controller unit telecommunication interface (**410**). In response to receiving the off hook indication, the communications processor can simulate the response to the off hook signal expected by the alarm controller unit (**420**). A "connection" will then be established between the alarm controller unit's telecommunication interface and the communications processor (**430**), for example, by the communications processor simulating responses that the alarm controller unit would expect to receive from a central monitoring service system (e.g., a handshake signal).

The alarm processor will then provide data related to the alarm condition that triggered the dial out. This data will be received from the alarm controller unit's telecommunications interface (**435**). Such data can be provided in a form of, for example, a set of dual tone multi-frequency signals (e.g., tone dialing) or through a modem-like exchange. The received data can then be interpreted, for example, in accord with the ContactID format (**440**). As with FIG. **3**, a determination can be made as to whether a communication mode for communicating over an external network to a remote server has been selected (**450**). If a communication mode has not been selected, then a communication mode can be selected from among the available communication modes, as discussed above (**455**). Once a communication mode has been selected, a signal can be generated in the protocol of the selected communication mode that includes the information received from the telephone interface (**460**). The generated signal can then be transmitted to the external network via the selected communication mode. In this manner, alarm conditions can be supplied to a remote server system coupled to the selected external network.

FIG. **5** is a simplified flow diagram illustrating steps performed in providing control information generated by a remote server to a legacy alarm system, in accord with embodiments of the present invention. For example, in response to a user command or for network system maintenance, a remote server (e.g., **270**) can generate a signal containing control information for the legacy alarm system. The remote server can transmit that information to the control unit via a communication mode selected by the remote server. While the remote server can be periodically provided with information related to the communication unit's selected communication mode (as well as other status information related to the communication unit), the remote server can itself determine a preferred communication mode and use that mode. The remote server can track and provide information regarding the communication unit's selected communication mod

A signal from the remote server containing the control information can be received (**510**). The received signal can then be interpreted to determine the nature of the control information contained in the signal (**520**). The interpreted information can then be transmitted to the keypad bus using a signal formatted for the appropriate keypad bus protocol (**530**).

As stated above, the remote server system (e.g., remote server system **270**) is a computer system coupled to a network external to communications unit **210**. The remote server system can receive status and alarm information from the communications unit and store and/or communicate the received status or alarm information to a user of the alarm system or to a monitoring station (e.g., a central station at which an operator can determine the appropriate authorities to contact based upon the nature of an alarm condition). The remote server system can also provide control information to the communications unit, including, for example, configuration information and updates to the communications unit and/or the alarm system. The remote server system can be configured to respond to the various status and/or alarm conditions by the user of the alarm system or an administrator of the remote server system, as discussed more fully below.

FIG. **6** is a simplified flow diagram illustrating a method followed by a remote server system in response to receiving data from a communications unit, in accord with embodiments of the present invention. The remote server system can receive data transmitted by a communications unit (e.g., **210**) (**610**). The data will be received by the remote server system over a communication mode selected by the communication unit, as discussed above.

The data received can correspond to, for example, status information related to alarm controller unit **110** or communications unit **210**, or alarm information related to a security breach. The remote server system will analyze the received data to determine whether the data contains reportable information, such as an alarm condition (**620**). If the data is related to reportable information, the server system will determine the nature of the reportable information (e.g., an alarm condition such as a fire or an unauthorized breach of a zone) (**625**). Based upon that determination, the remote server system can then contact a monitoring station to appraise an operator of the monitoring system, or an automated system, of the nature of the reportable information (**630**). Should the data received from the communication unit not contain reportable information, then the remote server system can determine the type of event described by the received data (**640**).

In either situation (reportable or non-reportable event), the remote server system can then identify a proper response to the event type described by the received data (**650**). Such an identification of a proper response can be performed through a search of a set of responses stored by the remote server system each of which are mapped to one or more event types. The set of responses can be defined, at least in part, by the user of the alarm system or an administrator of the remote server system. The remote server system can enable an authorized user to log on and can provide an interface (e.g., a set of web browser pages using, for example, HTML or XML or applets) through which the various responses can be added, deleted, or modified. For example, a user can configure the remote server system to alert a specified person when the remote server system receives data from the communications unit indicating that a specified disarm sequence has been provided through a keypad. Such an alert to the user can be provided by a specified communication path (e.g., electronic mail, text message, instant message, telephone or cellular phone call, RSS feed, a web page update or an applet).

Once a proper response to an event type is identified, the remote server system can then perform the identified response (**660**). For example, the remote server system can contact identified individuals and inform them of the nature of an event type, using a chosen communication delivery method such as electronic mail, text or instant messages, telephone calls, or an update to a web page or applet. The remote server system can also be configured to accept inputs from a user or administrator that correspond to control information for the alarm system controller unit (e.g., **110**) or the communications unit (e.g., **210**). An authorized user for a particular alarm system can access interfaces provided by the remote server system for entering such control information (e.g., web pages). The remote server system can then interpret the control information and provide that information to the communications unit over a communications mode selected by the remote server system. The communications unit will then receive that control information and provide the control information, as appropriate, to the alarm system controller unit as discussed above with regard to FIG. **5**. An example of control information that can be provided by a user to the alarm system via the remote server system can include remotely arming or disarming the alarm system.

One of the advantages of the present invention is that the communication unit provides two-way communication over a plurality of communication modes to a legacy alarm system. Thus, without replacing the legacy alarm system, a user of the system gains added functionality such as redundant connectivity and the ability to monitor and remotely control the legacy alarm system. Such an addition of functionality, rather than a whole scale replacement of an alarm system, can be provided at a substantially lower cost than replacing the system.

FIG. **7** is a simplified block diagram illustrating one example of a connection between a communication unit **210** and a legacy alarm system controller unit **110**. Typically, a legacy alarm system controller is housed in a wall-mounted metal housing **710**. Such an alarm system controller housing will typically have a key-lockable door (not shown) in order to restrict access to the circuitry and connections inside. One embodiment of a communications unit of the present invention can be housed in a housing **720** that can be attached to the alarm control unit housing **710**. Coupling between communications unit housing **720** and alarm control unit housing **710** can be performed by creating a hole in the alarm control unit's housing (typically by cutting out a pre-etched punch out in the housing) and passing through that hole a connector **730** that is rigidly mounted to the exterior of the communication unit housing and securing that connector to the alarm control unit's housing **710** (e.g., through use of a nut **735** threaded on the connector). Connector **730** can allow for passage into alarm control unit housing **710** of a cable **740** that includes necessary connector wires for coupling the communications unit to, for example, alarm system power, the keypad bus, and the telecommunications link to the alarm processor (all coupled to an alarm printed circuit board **750**), and the telephone line interface **760**. Typically, connections can be made to the alarm system power, keypad bus, etc. through already present screw down connections coupled to the alarm printed circuit board, or to modular jack connections (e.g., the telephone line interface). For ease of providing such connections, cable **740** can terminate in a hub **770** that provides connectors for the various coupling lines to the alarm printed circuit board **750** and telephone line interface **760**. Thus, connection of a communications unit to the alarm system can be performed by a homeowner, rather than a paid installer, thereby further reducing the cost, both to the user and to a supplier of the communications unit.

Embodiments of the present invention therefore provide a cost-effective solution for providing a legacy alarm system with a capacity to communicate over a selected one of a plurality of communication modes, thereby avoiding a single point of failure of many legacy alarm systems, and provides the added functionality of two-way communication from a remote server allowing control over the legacy alarm system from a location other than within the premises in which the alarm system is installed.

An Example Computing Environment

As shown above, the present invention can be implemented using a variety of computer systems, for example with regard to server system **270**. An example of one such computing environment is described below with reference to FIG. **8**.

FIG. **8** depicts a block diagram of a computer system **810** suitable for implementing embodiments of the present invention. Computer system **810** includes a bus **812** which interconnects major subsystems of computer system **810**, such as a central processor **814**, a system memory **817** (typically RAM, but which may also include ROM, flash RAM, or the like), an input/output controller **818**, an external audio device, such as a speaker system **820** via an audio output interface **822**, an external device, such as a display screen **824** via display adapter **826**, serial ports **828** and **830**, a keyboard **832** (interfaced with a keyboard controller **833**), a storage interface **834**, a floppy disk drive **837** operative to receive a floppy disk **838**, a host bus adapter (HBA) interface card **835**A operative to connect with a Fibre Channel network **890**, a host bus adapter (HBA) interface card **835**B operative to connect to a SCSI bus **839**, and an optical disk drive **840** operative to receive an optical disk **842**. Also included are a mouse **846** (or other point-and-click device, coupled to bus **812** via serial port **828**), a modem **847** (coupled to bus **812** via serial port **830**), and a network interface **848** (coupled directly to bus **812**).

Bus **812** allows data communication between central processor **814** and system memory **817**, which may include read-only memory (ROM) or flash memory (neither shown), and random access memory (RAM) (not shown), as previously noted. The RAM is generally the main memory into which the operating system and application programs are loaded. The ROM or flash memory can contain, among other code, the Basic Input-Output system (BIOS) which controls basic hardware operation such as the interaction with peripheral components. Applications resident with computer system **810** are generally stored on and accessed via a computer readable medium, such as a hard disk drive (e.g., fixed disk **844**), an optical drive (e.g., optical drive **840**), a floppy disk unit **837**, or other storage medium. Additionally, applications can be in the form of electronic signals modulated in accordance with the application and data communication technology when accessed via network modem **847** or interface **848**.

Storage interface **834**, as with the other storage interfaces of computer system **810**, can connect to a standard computer readable medium for storage and/or retrieval of information, such as a fixed disk drive **844**. Fixed disk drive **844** may be a part of computer system **810** or may be separate and accessed through other interface systems. Modem **847** may provide a direct connection to a remote computer, or a communications unit **210**, via a telephone link through a PSTN. Network interface **848** may provide a direct connection to a remote computer, or a communications unit **210**, via a direct network link to the Internet via a POP (point of presence). Network interface **848** may provide such connection using wireless techniques, including digital cellular telephone connection, Cellular Digital Packet Data (CDPD) connection, digital satellite data connection or the like.

Many other devices or subsystems (not shown) may be connected in a similar manner (e.g., document scanners, digital cameras and so on). Conversely, all of the devices shown in FIG. **8** need not be present to practice the present invention. The devices and subsystems can be interconnected in different ways from that shown in FIG. **8**. The operation of a computer system such as that shown in FIG. **8** is readily known in the art and is not discussed in detail in this application. Code to implement the present invention can be stored in computer-readable storage media such as one or more of system memory **817**, fixed disk **844**, optical disk **842**, or floppy disk **838**. The operating system provided on computer system **810** may be MS-DOS®, MS-WINDOWS®, OS/2®, UNIX®, Linux®, or another known operating system.

Moreover, regarding the signals described herein, those skilled in the art will recognize that a signal can be directly transmitted from a first block to a second block, or a signal can be modified (e.g., amplified, attenuated, delayed, latched, buffered, inverted, filtered, or otherwise modified) between the blocks. Although the signals of the above described embodiment are characterized as transmitted from one block to the next, other embodiments of the present invention may include modified signals in place of such directly transmitted signals as long as the informational and/or functional aspect of the signal is transmitted between blocks. To some extent, a signal input at a second block can be conceptualized as a second signal derived from a first signal output from a first block due to physical limitations of the circuitry involved (e.g., there will inevitably be some attenuation and delay). Therefore, as used herein, a second signal derived from a first signal includes the first signal or any modifications to the first signal, whether due to circuit limitations or due to passage through other circuit elements which do not change the informational and/or final functional aspect of the first signal.

Other Embodiments

The present invention is well adapted to attain the advantages mentioned as well as others inherent therein. While the present invention has been depicted, described, and is defined by reference to particular embodiments of the present invention, such references do not imply a limitation on the invention, and no such limitation is to be inferred. The invention is capable of considerable modification, alteration, and equivalents in form and function as will occur to those ordinarily skilled in the pertinent arts. The depicted and described embodiments are examples only, and are not exhaustive of the scope of the invention.

The foregoing describes embodiments including components contained within other components (e.g., the various elements shown as components of communications unit **210**). Such architectures are merely examples, and, in fact, many other architectures can be implemented which achieve the same functionality. In an abstract but still definite sense, any arrangement of components to achieve the same functionality is effectively "associated" such that the desired functionality is achieved. Hence, any two components herein combined to achieve a particular functionality can be seen as "associated with" each other such that the desired functionality is achieved, irrespective of architectures or intermediate components. Likewise, any two components so associated can also be viewed as being "operably connected" or "operably coupled" to each other to achieve the desired functionality.

The foregoing detailed description has set forth various examples of the present invention via the use of block diagrams, flow charts, and examples. It will be understood by those within the art that each block diagram component, flow chart step, operation and/or component illustrated by the use of examples can be implemented, individually and/or collectively, by a wide range of hardware, software, firmware, or any combination thereof.

The above description is intended to be illustrative of the invention and should not be taken to be limiting. Other embodiments within the scope of the present invention are possible. Those skilled in the art will readily implement the steps necessary to provide the structures and the methods disclosed herein, and will understand that the process parameters and sequence of steps are given by way of example only and can be varied to achieve the desired structure as well as modifications that are within the scope of the invention. Variations and modifications of the embodiments disclosed herein can be made based on the description set forth herein, without departing from the scope of the invention.

Consequently, the invention is intended to be limited only by the scope of the appended claims, giving full cognizance to equivalence in all respects.

Although the present invention has been described in connection with several embodiments, the invention is not intended to be limited to the specific forms set forth herein. On the contrary, it is intended to cover such alternatives, modifications, and equivalents as can be reasonably included within the scope of the invention as defined by the appended claims.

What is claimed is:

1. A system comprising:

a communications unit, coupled to a keypad bus of an alarm system controller unit and an external network via a plurality of communication modes, and configured to receive a first signal on the keypad bus from the alarm systems controller unit,

select a communication mode of the plurality of communication modes to communicate to the external network, and

transmit a first set of data comprising information from the first signal to the external network over the selected communication mode; and

a network server coupled to the external network and configured to receive the first set of data transmitted by the communications unit, and perform a pre-determined response to the information in the first set of data.

2. The system of claim **1** further comprising:

the communications unit further coupled to an alarm processor of the alarm system controller unit via a telecommunications interface; and

the communications unit further configured to

receive a second signal over the telecommunications interface, and

transmit a second set of data comprising information from the second signal to the external network over the selected communication mode.

3. The system of claim **2** further comprising:

the network server further configured to

receive the second set of data transmitted by the communications unit, and

perform a pre-determined response to information in the second set of data.

4. The system of claim **3** further comprising:

the network server further configured to

determine whether the information in the first or second set of data comprises reportable information to provide to a monitoring station, and if the information in the first or second set of data comprises reportable information, provide a description corresponding to the reportable information to the monitoring station.

5. The system of claim **1** further comprising:

the network server further configured to

store a set of responses to information received from the communications unit, wherein

the information comprises one of a plurality of events and conditions reported by the alarm system controller unit or a device coupled to the keypad bus, and

each response of the set of responses corresponds to an event or condition of the plurality of events and conditions, and

select the pre-determined response to the information in the first set of data from the set of responses.

6. The system of claim **5** wherein the pre-determined response comprises providing a description corresponding to the information in the first set of data to a selected user.

7. The system of claim **6** further comprising:

the network server further configured to

perform said providing the description by transmitting an electronic mail message to the selected user.

8. The system of claim **6** further comprising:

the network server further configured to

perform said providing the description by transmitting an SMS text message to the selected user.

9. The system of claim **6** further comprising:

the network server further configured to

perform said providing the description by providing information viewable by a web browser.

10. The system of claim **6** further comprising:

the network server further configured to

perform said providing the description by initiating a telephone call to the selected user and transmitting an audible message.

11. The system of claim **6** further comprising:

the network server further configured to

perform said providing the description by causing an instant message (IM) to be transmitted to an IM receiver.

12. The system of claim **6** further comprising:

the network server further configured to

perform said providing the description by causing a really simple syndication (RSS) feed to be transmitted to an RSS receiver.

13. The system of claim **5** further comprising:

the network server further configured to

enable a user to enter response data, and

store the response data as a response of the set of responses.

14. The system of claim **13** wherein enabling the user to enter response data comprises:

authorizing the user to access the set of responses corresponding to the communications unit.

15. The system of claim **1** further comprising:

the network server further configured to

transmit control information to the communication unit over the selected communication mode; and

the communications unit further configured to

receive the control information, and

transmit control data corresponding to the received control information to the alarm system controller unit over the keypad bus.

16. The system of claim **15** further comprising:

the network server further configured to

receive control input from a user, and

in response to the control input, generate the control information.

* * * * *

EXHIBIT 2

US007956736B2

(12) **United States Patent**
Cohn et al.

(10) **Patent No.: US 7,956,736 B2**
(45) **Date of Patent: *Jun. 7, 2011**

(54) **METHOD AND SYSTEM FOR COMMUNICATING WITH AND CONTROLLING AN ALARM SYSTEM FROM A REMOTE SERVER**

(75) Inventors: **Alan Wade Cohn**, Austin, TX (US); **Ronald E. Battles**, Cedar Park, TX (US); **David Proft**, Austin, TX (US); **Scott William Shumate**, Austin, TX (US)

(73) Assignee: **uControl, Inc.**, Austin, TX (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 12 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **12/620,047**

(22) Filed: **Nov. 17, 2009**

(65) **Prior Publication Data**

US 2010/0066530 A1 Mar. 18, 2010

Related U.S. Application Data

(63) Continuation of application No. 11/711,972, filed on Feb. 28, 2007, now Pat. No. 7,633,385.

(51) **Int. Cl.**
G08B 29/00 (2006.01)
G08B 9/00 (2006.01)

(52) **U.S. Cl.** **340/506**; 340/286.02

(58) **Field of Classification Search** 340/500–513, 340/541–567, 691.1–691.6, 693.5–693.12, 340/3.2–3.32, 3.7, 3.9, 825.36–7.61, 286.01, 340/286.02, 815.48, 815.49; 341/22, 26; 709/218, 224, 225; 706/22, 23
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,951,029	A	8/1990	Severson	340/506
5,134,644	A	7/1992	Garton et al.	379/39
5,438,607	A	8/1995	Przygoda, Jr. et al.	379/38
5,499,014	A	3/1996	Greenwaldt	340/539
5,625,338	A	4/1997	Pildner et al.	340/539
5,717,379	A	2/1998	Peters	340/539
5,777,551	A	7/1998	Hess	340/541
5,892,442	A	4/1999	Ozery	340/539
5,943,394	A	8/1999	Ader et al.	379/40
6,032,036	A	2/2000	Maystre et al.	455/404
6,038,289	A	3/2000	Sands	379/26
6,049,272	A	4/2000	Lee et al.	340/539

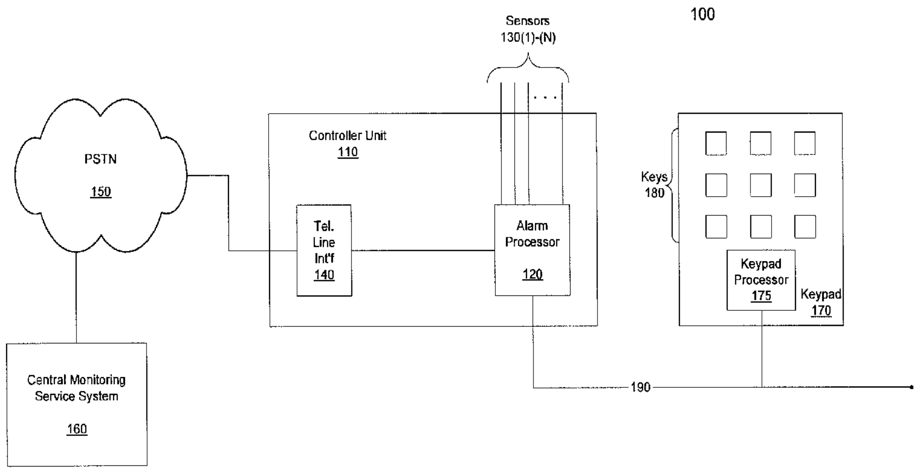
(Continued)

Primary Examiner — Jennifer Mehmood
(74) *Attorney, Agent, or Firm* — Campbell Stephenson LLP

(57) **ABSTRACT**

A communication system is provided that can be added to a legacy alarm system to provide a plurality of communication modes to a remote server system from the legacy alarm system and provide remote control and monitoring to a user of the system via two-way communication links. The communication system can be configured to communicate with an alarm processor of the legacy alarm system through use of a keypad bus typically used by the legacy alarm system for communication between the alarm processor and one or more keypads. Communication modes that can be provided by embodiments of the present invention can include, for example, communication over a public switched telephone network, cellular transmission, broadband transmission, and the like. The communication system can monitor all configured communication modes and determine which communication mode is the best for providing communication between the alarm system and the remote server. Through these communication modes and by virtue of being coupled to the alarm processor via the keypad bus, the communication system can provide both transmission to the remote server of the status and alarm condition of the legacy alarm system as well as provide control signals from the remote server to the legacy alarm system. The remote server provides pre-determined responses to information received from the alarm system, including providing alarm system condition information to a user or a monitoring station for response.

16 Claims, 8 Drawing Sheets



U.S. PATENT DOCUMENTS

6,049,273	A	4/2000	Hess	340/539
6,052,052	A	4/2000	Delmonaco	340/539
6,067,346	A	5/2000	Akhteruzzaman et al.	379/39
6,433,683	B1	8/2002	Robinson	340/540
6,661,340	B1	12/2003	Saylor et al.	340/517
6,693,545	B2	2/2004	Brown et al.	340/573
6,956,477	B2	10/2005	Chun	340/541
7,053,764	B2	5/2006	Stilp	340/506
7,248,161	B2	7/2007	Spoltore et al.	340/539.14
2003/0061344	A1	3/2003	Monroe	709/224
2003/0062997	A1	4/2003	Naidoo et al.	340/531
2005/0024203	A1	2/2005	Wolfe	340/539.22
2005/0216580	A1	9/2005	Raji et al.	709/223
2007/0226182	A1	9/2007	Sobotka et al.	707/3
2008/0091793	A1	4/2008	Diroo et al.	709/217

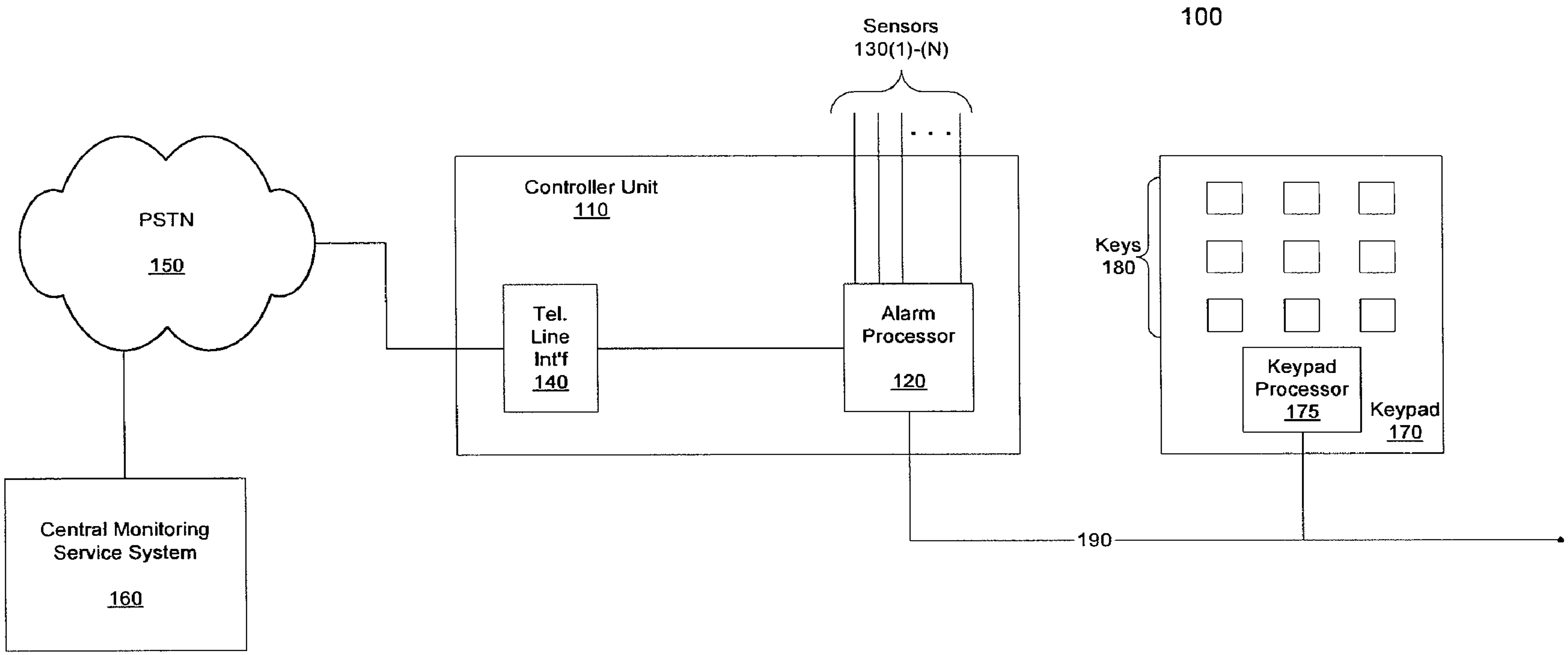

100
Sensors
130(1)-(N)
PSTN
150
Controller Unit
110
Tel.
Line
Int'f
140
Alarm
Processor
120
Keys
180
Keypad
Processor
175
Keypad
170
190
Central Monitoring
Service System
160

Figure 1

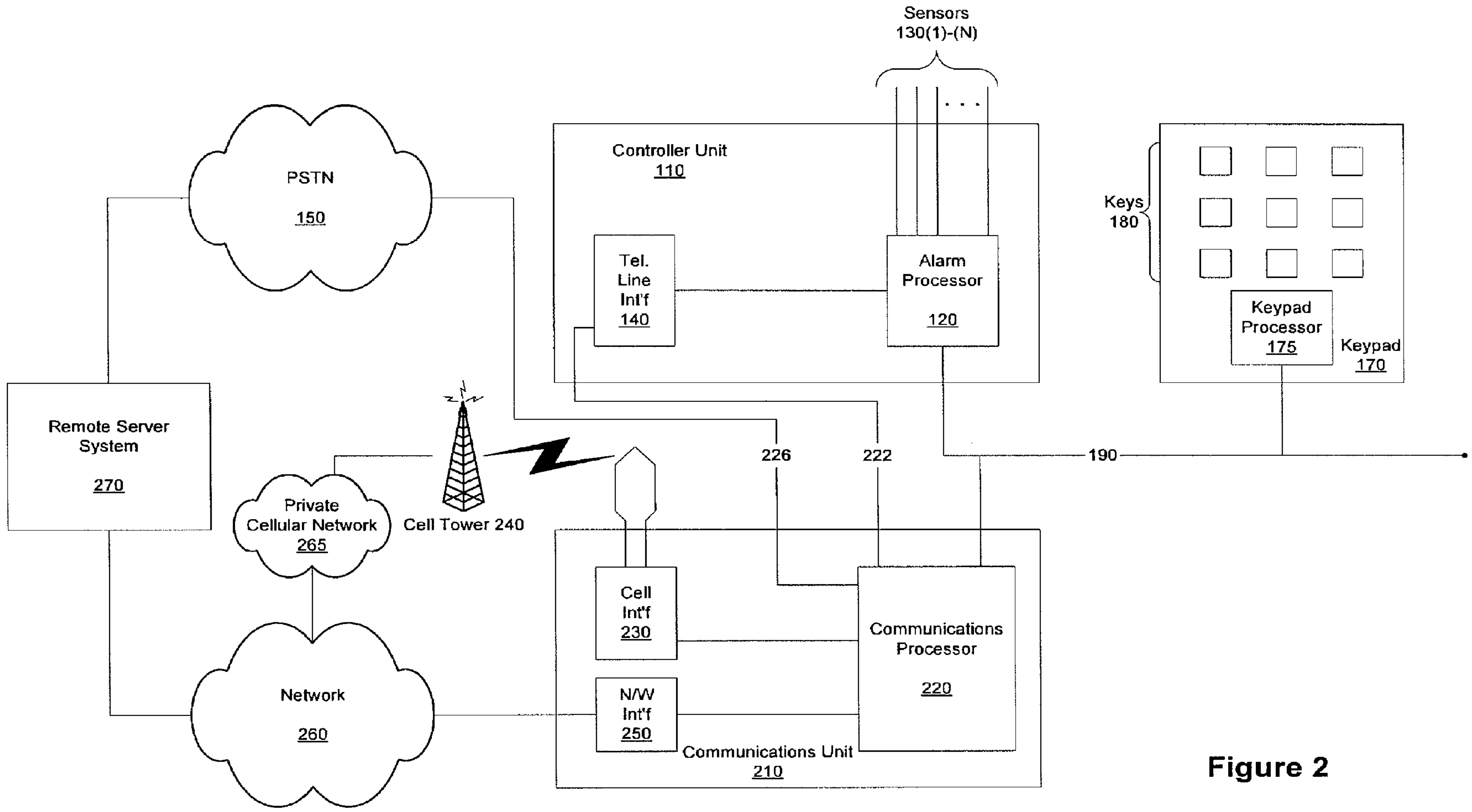

Sensors
130(1)-(N)
Controller Unit
110
PSTN
150
Tel.
Line
Int'f
140
Alarm
Processor
120
Keys
180
Keypad
Processor
175
Keypad
170
Remote Server
System
270
226
222
190
Private
Cellular Network
265
Cell Tower 240
Cell
Int'f
230
Communications
Processor
220
Network
260
N/W
Int'f
250
Communications Unit
210

Figure 2

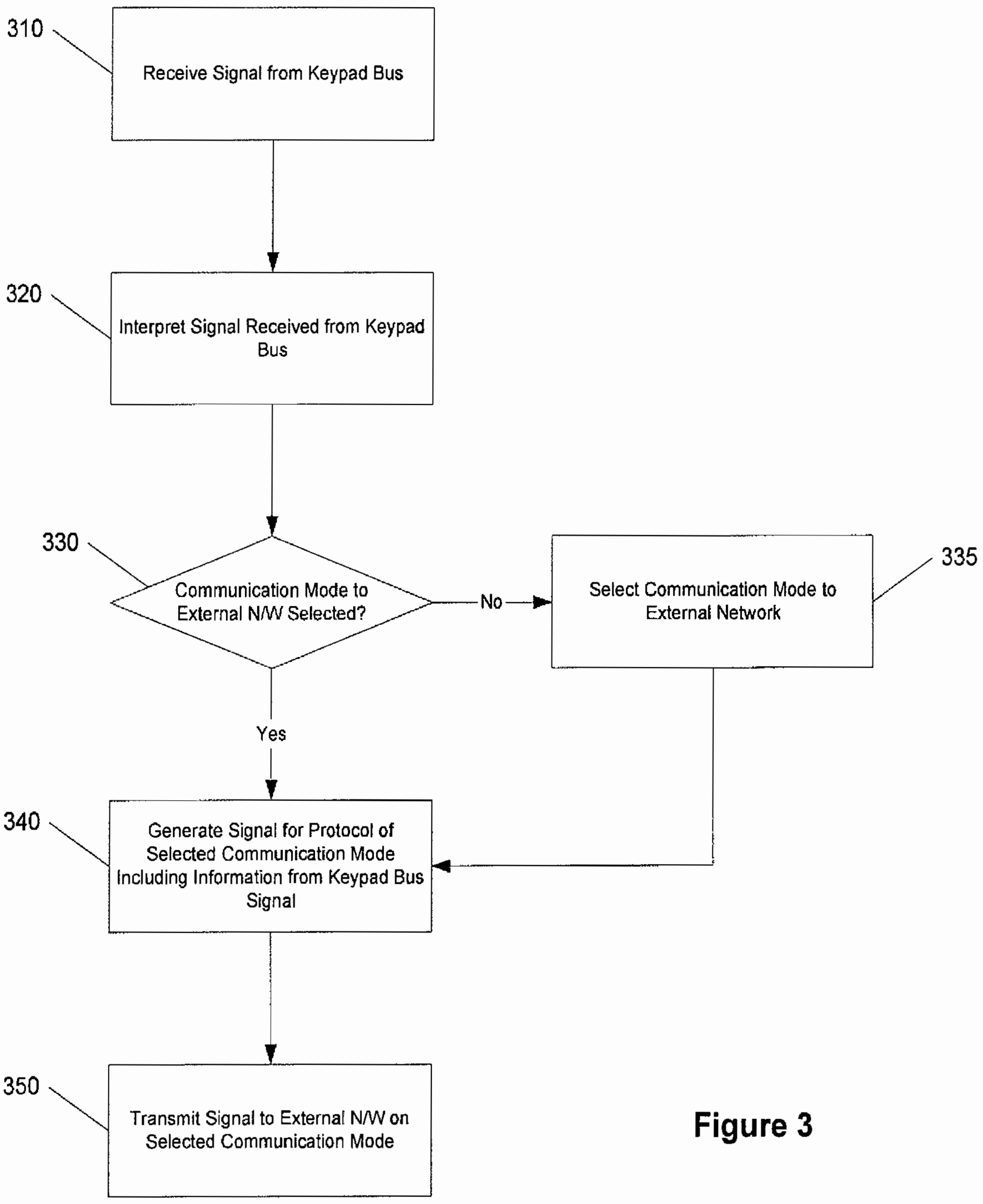

310
Receive Signal from Keypad Bus
320
Interpret Signal Received from Keypad Bus
330
Communication Mode to External N/W Selected?
No
335
Select Communication Mode to External Network
Yes
340
Generate Signal for Protocol of Selected Communication Mode Including Information from Keypad Bus Signal
350
Transmit Signal to External N/W on Selected Communication Mode

Figure 3

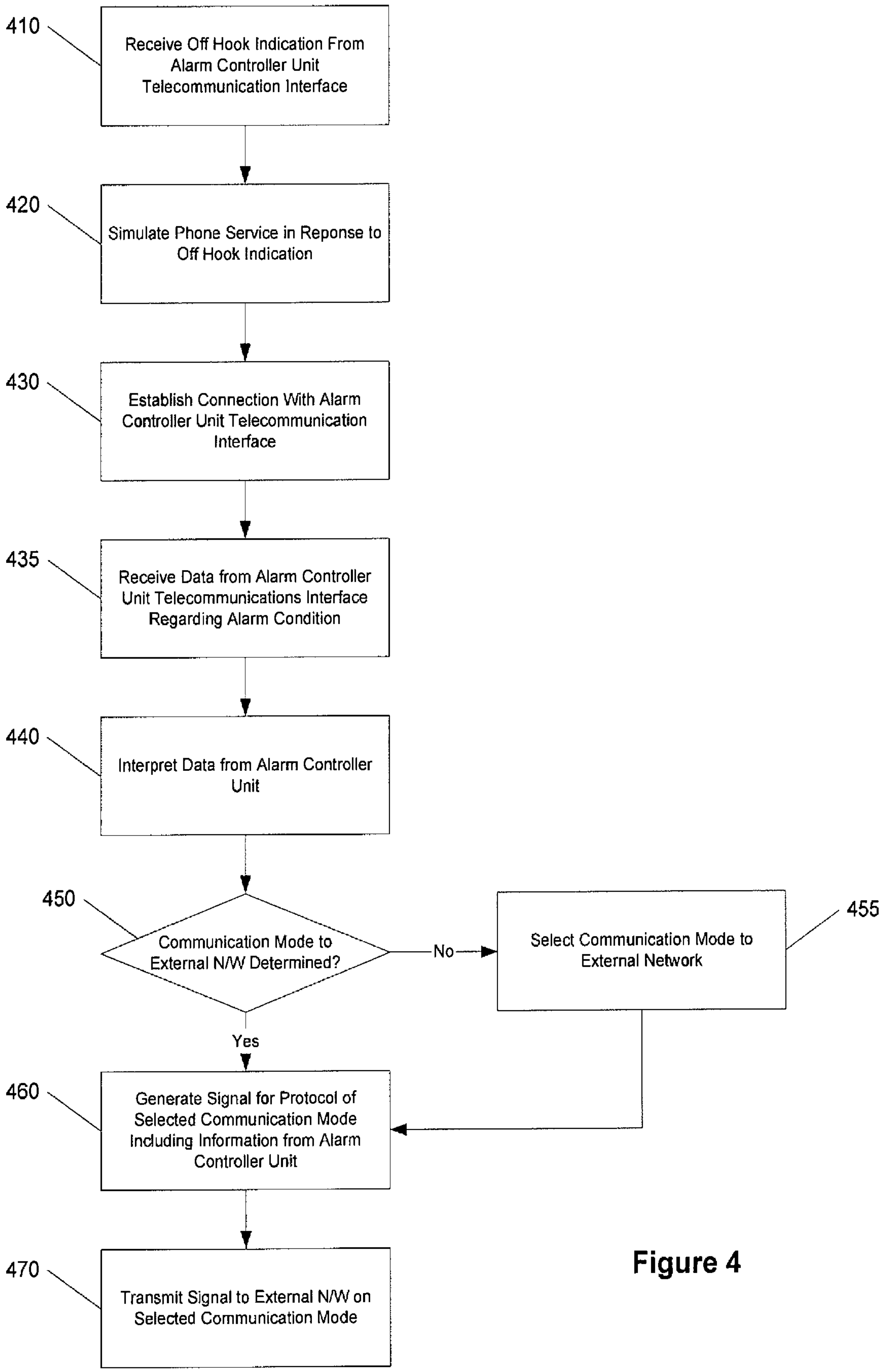

410
Receive Off Hook Indication From Alarm Controller Unit Telecommunication Interface
420
Simulate Phone Service in Reponse to Off Hook Indication
430
Establish Connection With Alarm Controller Unit Telecommunication Interface
435
Receive Data from Alarm Controller Unit Telecommunications Interface Regarding Alarm Condition
440
Interpret Data from Alarm Controller Unit
450
Communication Mode to External N/W Determined?
No
455
Select Communication Mode to External Network
Yes
460
Generate Signal for Protocol of Selected Communication Mode Including Information from Alarm Controller Unit
470
Transmit Signal to External N/W on Selected Communication Mode

Figure 4

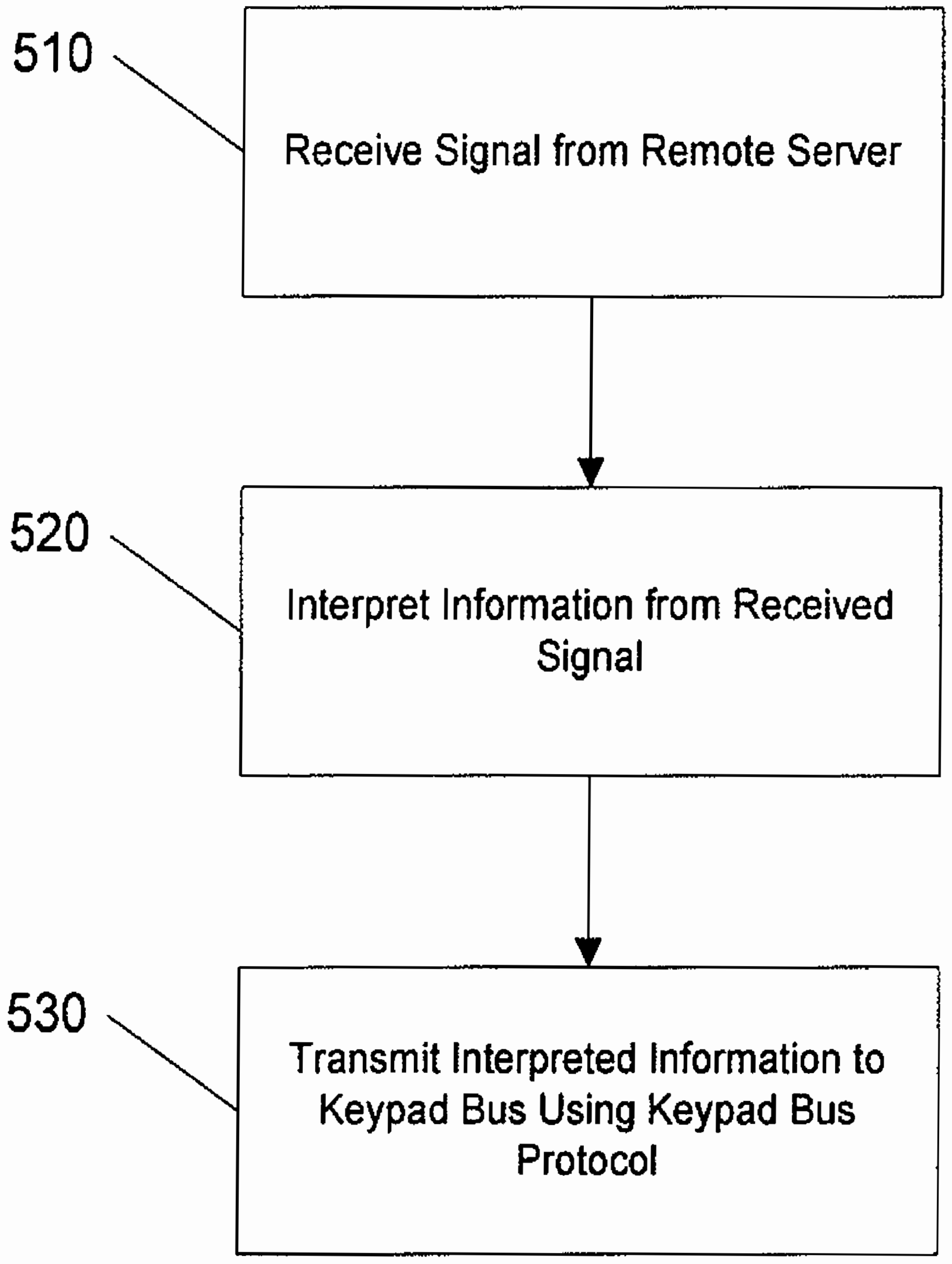

510
Receive Signal from Remote Server
520
Interpret Information from Received Signal
530
Transmit Interpreted Information to Keypad Bus Using Keypad Bus Protocol

Figure 5

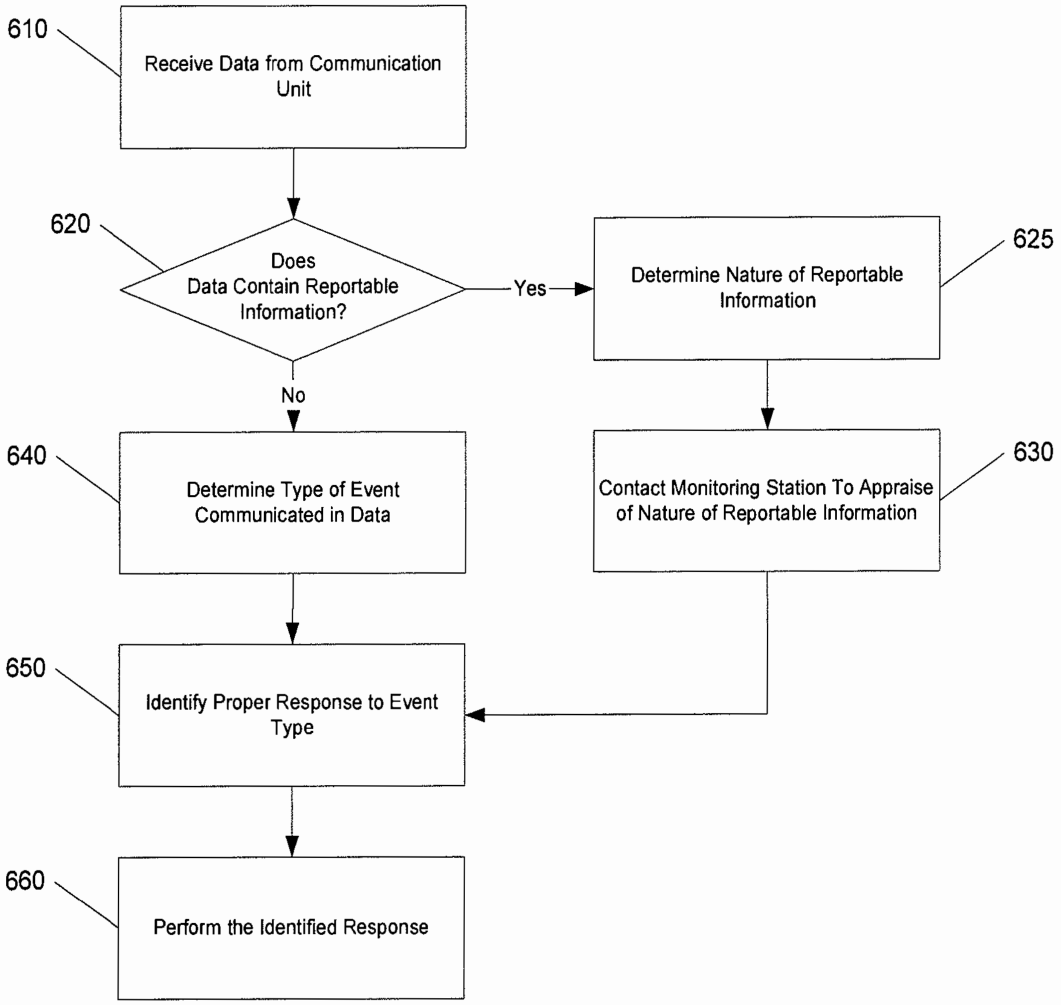

610
Receive Data from Communication Unit
620
Does Data Contain Reportable Information?
Yes
No
625
Determine Nature of Reportable Information
630
Contact Monitoring Station To Appraise of Nature of Reportable Information
640
Determine Type of Event Communicated in Data
650
Identify Proper Response to Event Type
660
Perform the Identified Response

Figure 6

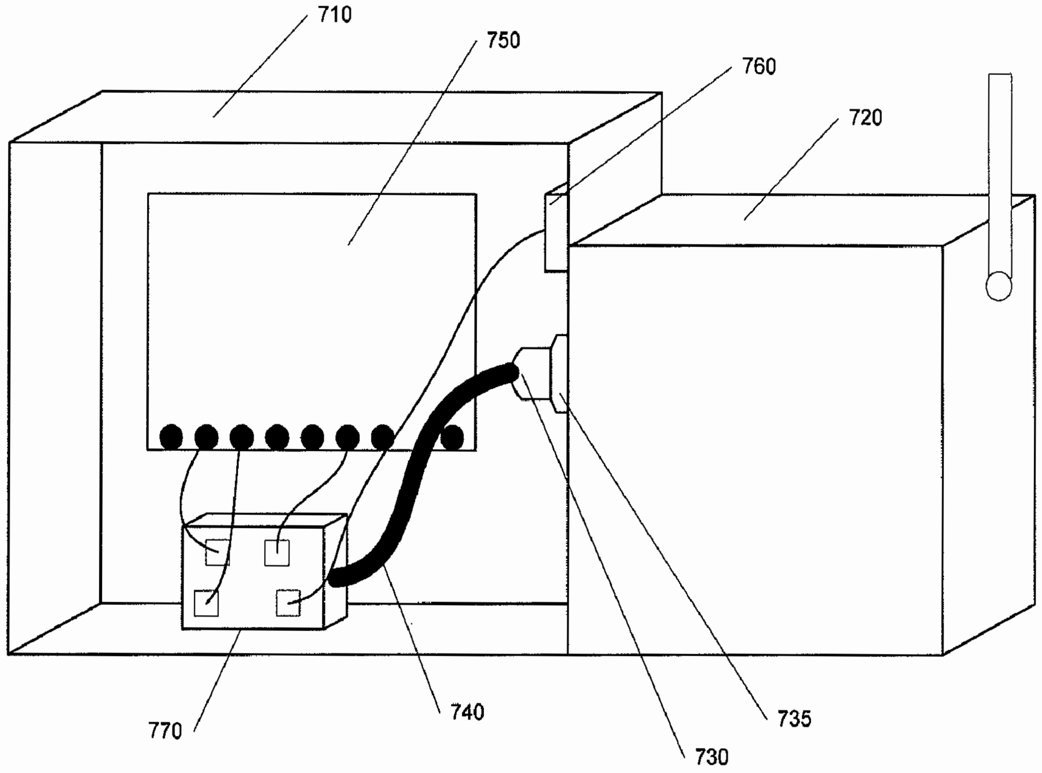

710
750
760
720
770
740
735
730

Figure 7

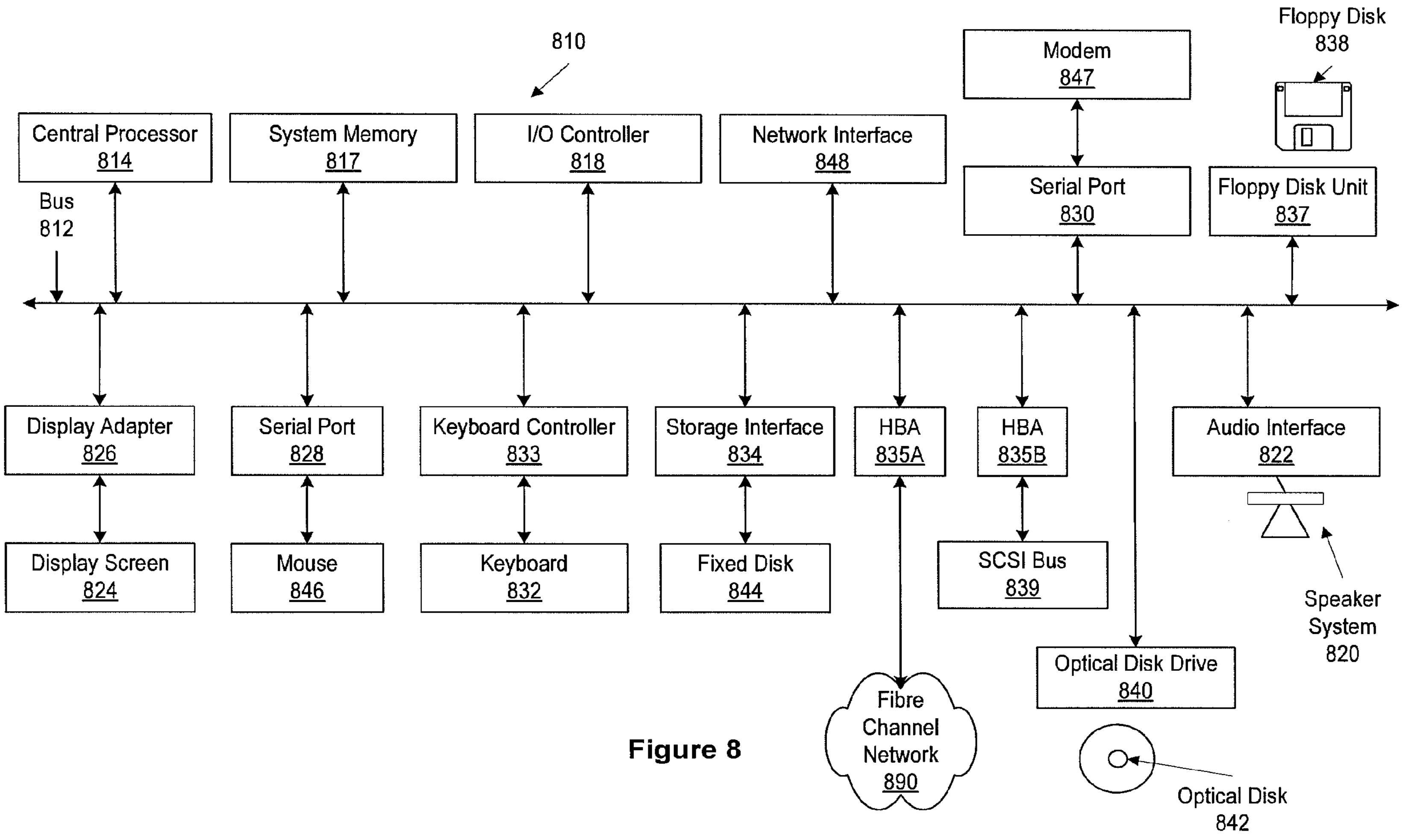

810
Central Processor
814
System Memory
817
I/O Controller
818
Network Interface
848
Modem
847
Serial Port
830
Floppy Disk
838
Floppy Disk Unit
837
Bus
812
Display Adapter
826
Serial Port
828
Keyboard Controller
833
Storage Interface
834
HBA
835A
HBA
835B
Audio Interface
822
Display Screen
824
Mouse
846
Keyboard
832
Fixed Disk
844
SCSI Bus
839
Speaker
System
820
Optical Disk Drive
840
Fibre
Channel
Network
890
Optical Disk
842

Figure 8

METHOD AND SYSTEM FOR COMMUNICATING WITH AND CONTROLLING AN ALARM SYSTEM FROM A REMOTE SERVER

CROSS REFERENCE TO RELATED APPLICATIONS

This application is a continuation of U.S. patent application Ser. No. 11/711,972, entitled "Method and System for Communicating with and Controlling an Alarm System from a Remote Server", filed Feb. 28, 2007 now U.S. Pat. No. 7,633,385, and naming Alan Wade Cohn, Ronald E. Battles, David Proft, and Scott William Shumate as inventors. This application is hereby incorporated by reference, in its entirety and for all purposes.

FIELD OF THE INVENTION

The present invention relates to the field of security systems, and more particularly relates to coupling a legacy alarm system to a server coupled to an external network via a plurality of monitored communication modes, enabling the server to provide control information to the legacy alarm system, and the legacy alarm system to report status and alarm conditions to the server.

BACKGROUND OF THE INVENTION

Security systems alert occupants of a dwelling and emergency authorities of a violation of premises secured by the security system. A typical security system includes a controller connected by wireless or wired connections to sensors deployed at various locations throughout the secured dwelling. In a home, sensors are usually deployed in doorways, windows, and other points of entry. Motion sensors can also be placed strategically within the home to detect unauthorized movement, while smoke and heat sensors can detect the presence of fire.

Security systems are usually connected to a central monitoring service system via a telecommunications line coupled to a public switched telephone network (PSTN). The central monitoring service system can be maintained by a security service provider and continuously monitors all activated subscriber security systems for alarms. Sensor activity occurs when a sensor detects, for example, an opening of a door or window, or presence of movement, or a fire. Sensor activity causes the sensor to send a signal to the controller of the security system. Responsive to receiving the signal, the controller can determine whether the signal represents an alarm condition and, if so, issue an audible alarm to alert the occupants of the dwelling and can originate a data transmission to the central monitoring service system via the telecommunications line. Upon receiving notification of an alarm, the central monitoring service system can determine the type of activity, attempt to contact the dwelling occupants, and alert appropriate authorities of an emergency situation.

Typically, the telecommunications line interconnecting the security system to the central monitoring service system is the dwelling occupant's telephone line. This line usually emanates from and is accessible from the exterior of the dwelling. It is this telecommunications line which delivers a security breach signal to the central monitoring service system via a PSTN.

One drawback of such a security system is that the telecommunications line becomes a potential single point of failure for providing a security breach signal to the central monitoring service system. Should the telephone line be rendered inoperative, for example, by an intruder cutting the telecommunications line prior to attempting entry, or due to other types of telecommunications systems failure, then the security breach signal will fail to be provided to the central monitoring service system and further action, such as notification of the authorities will not occur. Such links between a security system and a central monitoring service system are typically one-way, providing only data from the security system to the central monitoring system, which is another drawback. Such a one-way communication link does not allow for remote access of the security system to monitor or control the system.

Other security systems exist that can provide either a redundant communication mode or two-way communication between the security system and a remote server, either accessed by a central monitoring service system or a user. The drawbacks with regard to these prior art systems are that should a dwelling already have a security system such as that described above, the legacy security system would have to be deinstalled and then replaced by a security system providing redundant communication modes and/or two-way communication. There is no capacity to add such functionality to an existing alarm system. Such replacement of a legacy security system entails high costs, as the controller unit of the legacy security system must be replaced, and the sensors need to be rewired to a new controller unit.

It is therefore desirable to provide a cost-effective solution for enabling legacy (pre-installed) security systems to be remotely controlled and monitored by either a user of the system (e.g., a home owner) or a central monitoring service system, through a plurality of continuously-monitored communication modes.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention may be better understood, and its numerous objects, features and advantages made apparent to those skilled in the art by referencing the accompanying drawings.

FIG. **1** is a simplified block diagram illustrating elements of an alarm system usable with embodiments of the present invention.

FIG. **2** is a simplified block diagram of components of a legacy alarm system coupled to a communications system, in accord with embodiments of the present invention.

FIG. **3** is a simplified flow diagram illustrating steps performed in providing a signal received from a keypad bus to an external network over a selected communication mode, in accord with embodiments of the present invention.

FIG. **4** is a simplified flow diagram illustrating steps for providing information in an alarm signal received from alarm processor's telephone interface to an external network, in accord with embodiments of the present invention.

FIG. **5** is a simplified flow diagram illustrating steps performed in providing control information generated by a remote server to a legacy alarm system, in accord with embodiments of the present invention.

FIG. **6** is a simplified flow diagram illustrating a method performed by a remote server system in response to receiving data from a communications unit, in accord with embodiments of the present invention.

FIG. **7** is a simplified block diagram illustrating one example of a connection between a communication unit and a legacy alarm system controller, in accord with embodiments of the present invention.

FIG. **8** depicts a block diagram of a computer system suitable for implementing embodiments of the present invention.

DETAILED DESCRIPTION

Embodiments of the present invention provide a communication system that can be added to a legacy alarm system to provide a plurality of communication modes to a remote server system from the legacy alarm system and provide remote control and monitoring to a user of the system via two-way communication links. Embodiments of the present invention can be configured to communicate with an alarm processor of the alarm system through use of a keypad bus typically used by the legacy alarm system for communications between the alarm processor and one or more keypads. Communication modes to the remote server system that can be provided by embodiments of the present invention can include, for example, communication over a public switched telephone network, cellular transmission, broadband transmission, and the like. Embodiments of the present invention can monitor all configured communication modes and determine which communication mode is the best for providing communication between the alarm system and the remote server. Through these communication modes and by virtue of being coupled to the alarm processor via the keypad bus, embodiments of the present invention can provide both transmission to the remote server of the status and alarm condition of the legacy alarm system as well as provide control signals from the remote server to the legacy alarm system.

FIG. **1** is a simplified block diagram illustrating elements of a legacy alarm system **100**. Alarm system **100** includes a controller unit **110**. Controller unit **110** includes an alarm processor **120**, which is coupled to sensors **130**(**1**)-(N). Sensors **130**(**1**)-(N) can be installed at various points of entry for a building to detect when such a point of entry is reached, and can also include, for example, motion, smoke, and fire detectors. Alarm processor **120** can define zones each of which can include one or more alarm sensors **130**(**1**)-(N). Alarm processor **120** is further coupled to a telephone line interface **140**. In the event of a triggering of one of sensors **130**(**1**)-(N), alarm processor **120** can instruct telephone line interface **140** to dial a call through public switched telephone network (PSTN) **150** to a central monitoring service system **160**. Alarm processor **120** can then send data through the connection to the central monitoring service system, providing information related to the type of security breach (e.g., identification of zone, fire or intrusion alarm, etc.).

Alarm processor **120** is also coupled to a keypad **170**. Keypad **170** allows a user in the building to control the alarm system by performing tasks such as arming and disarming the alarm system, activating an alarm sequence to activate an audible alarm and call to the central monitoring service system, sending a silent distress signal to the central monitoring service system, and programming and configuring alarm system **100**. Keypad **170** includes a keypad processor **175**, which is coupled to keys **180** through which the user can enter commands. Keypad **170** can also include, for example, visual indicators of the status of the alarm system such as LEDs or a display, which are coupled to the keypad processor. Alarm processor **120** is coupled to keypad processor **175** through a keypad bus **190**. Keypad bus **190** provides communication between the alarm processor and keypad processor using, for example, a serial digital protocol transmitted and received by the processors. One or more keypads can be connected to the alarm processor via the keypad bus.

Through the use of the keypad bus serial digital protocol, the alarm processor can provide to the keypad information such as whether the alarm is armed or disarmed, and whether zones are tripped or not. The keypad processor can provide arming codes and other control information to the alarm processor.

FIG. **2** is a simplified block diagram of components of a legacy alarm system coupled to a communications system in accord with embodiments of the present invention. As discussed above, alarm controller **110** includes a microprocessor **120** that is coupled to sensors **130**(**1**)-(N). Alarm processor **120** is coupled via keypad bus **190** to keypad processor **175** within keypad **170**. Communications unit **210** provides a communications processor **220** that is coupled to alarm processor **120** and keypad processor **175** via keypad bus **190**. Thus, communications processor **220** can exchange data with alarm processor **120** using the serial digital protocol of keypad bus **190**. Communications processor **220** can be configured to automatically determine the type of serial digital protocol being used in communications between alarm processor **120** and keypad processor **175** as part of an initial configuration of communications unit **210** upon being coupled to the keypad bus.

Communications processor **220** is also coupled to controller unit **110** via telecommunications link **222**, which is coupled to the outgoing port of telephone line interface **140**. Communications processor **220** is further coupled to PSTN **150** by telecommunications link **226**, thereby breaking the direct link between telephone line interface **140** and PSTN **150** illustrated in FIG. **1**. Communications processor **220** then serves as an intermediary between alarm unit **110** and PSTN **150**. It is through this link that communications processor **220** can provide communication from alarm controller unit **110** to a remote server system **270** via the PSTN, should that be a selected communication mode (as described below).

Remote server system **270** can be a network-coupled computer system that provides, in part, responsive communication to information received from communications unit **210**. Such responsive communication can be provided to, for example, the user of the alarm system (e.g., a homeowner) or to emergency responders to alarm conditions. Remote server system **270** can also provide communication to communications unit **210**, including, for example, configuration information and updates.

Communications processor **220** can also be coupled to a cellular interface **230** that can provide cellular transmission to a cell tower **240** that is also coupled, directly or indirectly, to a private cellular network **265**, which is further coupled to a network **260**. Through this link, communications processor **220** can provide a cellular transmission communication mode to server system **270**, which is also coupled to network **260**.

Communications processor **220** can also be coupled to a network interface **250**. Network interface **250** can provide a broadband connection to network **260** (e.g., the Internet), which is also coupled to server system **270**. Through network interface **250**, communications processor **220** can provide a broadband communications mode to server system **270**.

In alternate embodiments of communications unit **210**, communications processor **220** can be coupled to other communication interfaces that can provide wireless broadband, Wi-Fi communication, and the like.

The multiple communication modes provided by communication unit **210** avoid the single point of failure (e.g., an external telephone line) present in legacy alarm systems. To this end, it is preferable that multiple communication modes not be transmitted over a common link from a building in which an alarm system is installed.

Communications processor **220** can monitor all of the available communication modes to determine which communication mode is the best for transmitting data to and from server system **270** at any point in time. For example, the communications processor, through network interface **250**, can monitor whether there is an active connection to network **260**. Such monitoring can be performed by, for example, by periodically establishing, or attempting to establish, a connection with server system **270** and monitoring a heartbeat signal. Alternatively, the communications processor can determine availability and viability of a network connection to the server system using, for example, network echo packets (e.g., pinging). Similarly, through cellular interface **230**, communications processor **220** can periodically establish, or attempt to establish, a connection with server system **270** through private cellular network **265** and network **260**. With regard to connections via PSTN **150**, the communications processor can, for example, determine whether there is an appropriate voltage over the telecommunications link **226** from the PSTN. In an event of a voltage drop on telecommunications link **226**, the communications processor can interpret such a drop as an event that needs to be communicated to the remote server (over either the broadband or cellular connection).

As the communications processor determines the best communication mode, that mode is then used for communication between communication unit **210** and server system **270** until a determination is made that an alternate communication mode is more appropriate. Alternatively, the communications processor can be configured to give primary preference to a particular communications mode (e.g., broadband), and then secondary preference to a different communications mode (e.g., cellular), and so on. In such a case, the communications processor will use the primary communications mode unless that communications mode is unavailable and then switch to a secondary (or lower) communications mode, depending upon availability of that mode.

An example communication mode configuration for the controller unit can provide for broadband being the primary communication mode, since broadband connections can be relatively inexpensive to maintain a constant link through and data rates are relatively high. The secondary communication mode can be a cellular connection because of difficulty involved in severing such a connection. But data rates may be lower for the cellular connection, as well as relatively more expensive. Thus, the communication unit can be configured, for example through control settings provided by server **270**, to only communicate a subset of events through cellular connections. To compensate for this reduced event data bandwidth, the communications unit can cache event information, along with time stamps, in a memory local to the communications unit and provide all those events to the server when the broadband connection is restored. Further, PSTN communication can be configured as a tertiary communication mode. Data rates through PSTN can determine a different subset of events reportable through PSTN, and again the communication unit can be configured with that subset. For example, data rates over PSTN can limit the communication unit to only transmit alarm event information over that communication mode. Alternatively, PSTN communication can result in some or all non-alarm, reportable events being cached for later transmission through the PSTN. Further, PSTN communication may limit communication unit-to-server communication to a one-way link, rather than two-way communication provided by broadband and cellular.

As stated above, communications processor **220** and alarm unit **110** are coupled over telecommunications link **222** in order for the communications processor to function as an intermediary between the alarm unit and PSTN **150**. In a legacy system, when alarm processor **120** detects an alarm situation, alarm processor **120** instructs telephone line interface **140** to dial out over PSTN **150** to communicate with the central monitoring service system. Communications processor **220** can simulate the phone service and the central monitoring system and interpret the alarm signals provided by alarm processor **120**. Alarm processor **120** provides such communication using, for example, a ContactID format. Communications processor **220** can read the data supplied by alarm processor **120** over the telecommunications link, interpret that data, and transmit an appropriate signal over the chosen communication mode to server system **270**.

Communications processor **220** can also interpret signals provided by alarm processor **120** over keypad bus **190**, and provide that information to server system **270** over the chosen communication mode. As stated above, such information can include arm/disarm indicators, zone trip information, system trouble (e.g., low battery, clock reset, no power), and the like.

As stated above, communications processor **220** interprets event signals received from alarm processor **120** over either keypad bus **190** or telephone line interface **140**. Communications processor **220** will then generate a signal to send over the selected communication mode to server system **270**. This signal corresponds to the interpretation of the event signal received from the alarm processor. In the case of alarm events received over the telephone line interface, the communications processor can also encapsulate original data received for transmission to the server system. In this manner, should the server system need to further analyze the alarm indication in order to determine a proper response, that data is provided in its original form.

Communications processor **220** can also receive information provided by server system **270** over a communication mode selected by the server system. Communications processor **220** can interpret that received information and format the information for the appropriate serial digital protocol of keypad bus **190**. Communications processor **220** can then provide the information to alarm processor **120** over keypad bus **190**. Through such communication, communications processor **220** emulates keypad communication to alarm processor **120**. Thus, there is no need to reprogram the legacy alarm system to allow the legacy alarm system to be controlled through communication unit **210**.

FIG. **3** is a simplified flow diagram illustrating steps performed in providing a signal received from a keypad bus to an external network over a communication mode, in accord with embodiments of the present invention. A data signal is received from a connection to a keypad bus (**310**), for example, by a communications processor **220**. Prior to receiving the signal, and typically upon initial startup of the communications unit when connected to the keypad bus, an identification of the serial digital protocol of the keypad bus is made. Such a determination of the keypad bus protocol can be made by one of several methods including, for example, analyzing the received data signal from the keypad bus and comparing that signal to expected signal formats for keypad bus protocols, or transmitting a test command from one of a plurality of possible keypad bus protocols and analyzing a received responsive signal for conformity with the protocol of the transmitted signal, or analyzing signals transmitted by a keypad **170** in response to a predetermined code entered into keys **180**, or analyzing timing parameters of the serial digital signal to determine the protocol type.

Using the determined keypad bus protocol, the signal received from the keypad bus can be interpreted (**320**). This interpretation can include determining the nature of the keypad bus signal (e.g., arm/disarm, zone tripped/not tripped, alarm controller status). A determination can then be made as to whether a communication mode to an external network has been previously selected (**330**). If not, then a selection of a communication mode to the external network can be made (**335**). As discussed above, the selection of a communication mode is made in response to periodic or continuous monitoring of the communication modes available to the communications unit. When a communication mode has been selected, a signal can then be generated corresponding to the protocol of the selected communication mode, wherein that signal includes information corresponding to the signal received from the keypad bus (**340**). That generated signal can then be transmitted to the external network via the selected communication mode (**350**). In order to perform such a transmission, it may be necessary to establish a link with the external network and ultimately to a remote server system coupled to the external network (e.g., **270**) in order to effect the data transfer.

FIG. **4** is a simplified flow diagram illustrating steps for providing information in an alarm signal received from alarm processor's telephone interface to an external network, in accord with embodiments of the present invention. As discussed above, upon detecting an alarm condition, such as a sensor breach, an alarm processor of a legacy alarm system will use a phone line to contact a central monitoring service system. Embodiments of the present invention are coupled to the telephone interface of the legacy alarm system and will receive an off hook indication generated by the alarm controller unit telecommunication interface (**410**). In response to receiving the off hook indication, the communications processor can simulate the response to the off hook signal expected by the alarm controller unit (**420**). A "connection" will then be established between the alarm controller unit's telecommunication interface and the communications processor (**430**), for example, by the communications processor simulating responses that the alarm controller unit would expect to receive from a central monitoring service system (e.g., a handshake signal).

The alarm processor will then provide data related to the alarm condition that triggered the dial out. This data will be received from the alarm controller unit's telecommunications interface (**435**). Such data can be provided in a form of, for example, a set of dual tone multi-frequency signals (e.g., tone dialing) or through a modem-like exchange. The received data can then be interpreted, for example, in accord with the ContactID format (**440**). As with FIG. **3**, a determination can be made as to whether a communication mode for communicating over an external network to a remote server has been selected (**450**). If a communication mode has not been selected, then a communication mode can be selected from among the available communication modes, as discussed above (**455**). Once a communication mode has been selected, a signal can be generated in the protocol of the selected communication mode that includes the information received from the telephone interface (**460**). The generated signal can then be transmitted to the external network via the selected communication mode. In this manner, alarm conditions can be supplied to a remote server system coupled to the selected external network.

FIG. **5** is a simplified flow diagram illustrating steps performed in providing control information generated by a remote server to a legacy alarm system, in accord with embodiments of the present invention. For example, in response to a user command or for network system maintenance, a remote server (e.g., **270**) can generate a signal containing control information for the legacy alarm system. The remote server can transmit that information to the control unit via a communication mode selected by the remote server. While the remote server can be periodically provided with information related to the communication unit's selected communication mode (as well as other status information related to the communication unit), the remote server can itself determine a preferred communication mode and use that mode. The remote server can track and provide information regarding the communication unit's selected communication mode.

A signal from the remote server containing the control information can be received (**510**). The received signal can then be interpreted to determine the nature of the control information contained in the signal (**520**). The interpreted information can then be transmitted to the keypad bus using a signal formatted for the appropriate keypad bus protocol (**530**).

As stated above, the remote server system (e.g., remote server system **270**) is a computer system coupled to a network external to communications unit **210**. The remote server system can receive status and alarm information from the communications unit and store and/or communicate the received status or alarm information to a user of the alarm system or to a monitoring station (e.g., a central station at which an operator can determine the appropriate authorities to contact based upon the nature of an alarm condition). The remote server system can also provide control information to the communications unit, including, for example, configuration information and updates to the communications unit and/or the alarm system. The remote server system can be configured to respond to the various status and/or alarm conditions by the user of the alarm system or an administrator of the remote server system, as discussed more fully below.

FIG. **6** is a simplified flow diagram illustrating a method followed by a remote server system in response to receiving data from a communications unit, in accord with embodiments of the present invention. The remote server system can receive data transmitted by a communications unit (e.g., **210**) (**610**). The data will be received by the remote server system over a communication mode selected by the communication unit, as discussed above.

The data received can correspond to, for example, status information related to alarm controller unit **110** or communications unit **210**, or alarm information related to a security breach. The remote server system will analyze the received data to determine whether the data contains reportable information, such as an alarm condition (**620**). If the data is related to reportable information, the server system will determine the nature of the reportable information (e.g., an alarm condition such as a fire or an unauthorized breach of a zone) (**625**). Based upon that determination, the remote server system can then contact a monitoring station to appraise an operator of the monitoring system, or an automated system, of the nature of the reportable information (**630**). Should the data received from the communication unit not contain reportable information, then the remote server system can determine the type of event described by the received data (**640**).

In either situation (reportable or non-reportable event), the remote server system can then identify a proper response to the event type described by the received data (**650**). Such an identification of a proper response can be performed through a search of a set of responses stored by the remote server system each of which are mapped to one or more event types. The set of responses can be defined, at least in part, by the user of the alarm system or an administrator of the remote server system. The remote server system can enable an authorized user to log on and can provide an interface (e.g., a set of web browser pages using, for example, HTML or XML or applets) through which the various responses can be added, deleted, or modified. For example, a user can configure the remote server system to alert a specified person when the remote server system receives data from the communications unit indicating that a specified disarm sequence has been provided through a keypad. Such an alert to the user can be provided by a specified communication path (e.g., electronic mail, text message, instant message, telephone or cellular phone call, RSS feed, a web page update or an applet).

Once a proper response to an event type is identified, the remote server system can then perform the identified response (**660**). For example, the remote server system can contact identified individuals and inform them of the nature of an event type, using a chosen communication delivery method such as electronic mail, text or instant messages, telephone calls, or an update to a web page or applet. The remote server system can also be configured to accept inputs from a user or administrator that correspond to control information for the alarm system controller unit (e.g., **110**) or the communications unit (e.g., **210**). An authorized user for a particular alarm system can access interfaces provided by the remote server system for entering such control information (e.g., web pages). The remote server system can then interpret the control information and provide that information to the communications unit over a communications mode selected by the remote server system. The communications unit will then receive that control information and provide the control information, as appropriate, to the alarm system controller unit as discussed above with regard to FIG. **5**. An example of control information that can be provided by a user to the alarm system via the remote server system can include remotely arming or disarming the alarm system.

One of the advantages of the present invention is that the communication unit provides two-way communication over a plurality of communication modes to a legacy alarm system. Thus, without replacing the legacy alarm system, a user of the system gains added functionality such as redundant connectivity and the ability to monitor and remotely control the legacy alarm system. Such an addition of functionality, rather than a whole scale replacement of an alarm system, can be provided at a substantially lower cost than replacing the system.

FIG. **7** is a simplified block diagram illustrating one example of a connection between a communication unit **210** and a legacy alarm system controller unit **110**. Typically, a legacy alarm system controller is housed in a wall-mounted metal housing **710**. Such an alarm system controller housing will typically have a key-lockable door (not shown) in order to restrict access to the circuitry and connections inside. One embodiment of a communications unit of the present invention can be housed in a housing **720** that can be attached to the alarm control unit housing **710**. Coupling between communications unit housing **720** and alarm control unit housing **710** can be performed by creating a hole in the alarm control unit's housing (typically by cutting out a pre-etched punch out in the housing) and passing through that hole a connector **730** that is rigidly mounted to the exterior of the communication unit housing and securing that connector to the alarm control unit's housing **710** (e.g., through use of a nut **735** threaded on the connector). Connector **730** can allow for passage into alarm control unit housing **710** of a cable **740** that includes necessary connector wires for coupling the communications unit to, for example, alarm system power, the keypad bus, and the telecommunications link to the alarm processor (all coupled to an alarm printed circuit board **750**), and the telephone line interface **760**. Typically, connections can be made to the alarm system power, keypad bus, etc. through already present screw down connections coupled to the alarm printed circuit board, or to modular jack connections (e.g., the telephone line interface). For ease of providing such connections, cable **740** can terminate in a hub **770** that provides connectors for the various coupling lines to the alarm printed circuit board **750** and telephone line interface **760**. Thus, connection of a communications unit to the alarm system can be performed by a homeowner, rather than a paid installer, thereby further reducing the cost, both to the user and to a supplier of the communications unit.

Embodiments of the present invention therefore provide a cost-effective solution for providing a legacy alarm system with a capacity to communicate over a selected one of a plurality of communication modes, thereby avoiding a single point of failure of many legacy alarm systems, and provides the added functionality of two-way communication from a remote server allowing control over the legacy alarm system from a location other than within the premises in which the alarm system is installed.

An Example Computing Environment

As shown above, the present invention can be implemented using a variety of computer systems, for example with regard to server system **270**. An example of one such computing environment is described below with reference to FIG. **8**.

FIG. **8** depicts a block diagram of a computer system **810** suitable for implementing embodiments of the present invention. Computer system **810** includes a bus **812** which interconnects major subsystems of computer system **810**, such as a central processor **814**, a system memory **817** (typically RAM, but which may also include ROM, flash RAM, or the like), an input/output controller **818**, an external audio device, such as a speaker system **820** via an audio output interface **822**, an external device, such as a display screen **824** via display adapter **826**, serial ports **828** and **830**, a keyboard **832** (interfaced with a keyboard controller **833**), a storage interface **834**, a floppy disk drive **837** operative to receive a floppy disk **838**, a host bus adapter (HBA) interface card **835**A operative to connect with a Fibre Channel network **890**, a host bus adapter (HBA) interface card **835**B operative to connect to a SCSI bus **839**, and an optical disk drive **840** operative to receive an optical disk **842**. Also included are a mouse **846** (or other point-and-click device, coupled to bus **812** via serial port **828**), a modem **847** (coupled to bus **812** via serial port **830**), and a network interface **848** (coupled directly to bus **812**).

Bus **812** allows data communication between central processor **814** and system memory **817**, which may include read-only memory (ROM) or flash memory (neither shown), and random access memory (RAM) (not shown), as previously noted. The RAM is generally the main memory into which the operating system and application programs are loaded. The ROM or flash memory can contain, among other code, the Basic Input-Output system (BIOS) which controls basic hardware operation such as the interaction with peripheral components. Applications resident with computer system **810** are generally stored on and accessed via a computer readable medium, such as a hard disk drive (e.g., fixed disk **844**), an optical drive (e.g., optical drive **840**), a floppy disk unit **837**, or other storage medium. Additionally, applications can be in the form of electronic signals modulated in accordance with the application and data communication technology when accessed via network modem **847** or interface **848**.

Storage interface **834**, as with the other storage interfaces of computer system **810**, can connect to a standard computer readable medium for storage and/or retrieval of information, such as a fixed disk drive **844**. Fixed disk drive **844** may be a part of computer system **810** or may be separate and accessed through other interface systems. Modem **847** may provide a direct connection to a remote computer, or a communications unit **210**, via a telephone link through a PSTN. Network interface **848** may provide a direct connection to a remote computer, or a communications unit **210**, via a direct network link to the Internet via a POP (point of presence). Network interface **848** may provide such connection using wireless techniques, including digital cellular telephone connection, Cellular Digital Packet Data (CDPD) connection, digital satellite data connection or the like.

Many other devices or subsystems (not shown) may be connected in a similar manner (e.g., document scanners, digital cameras and so on). Conversely, all of the devices shown in FIG. **8** need not be present to practice the present invention. The devices and subsystems can be interconnected in different ways from that shown in FIG. **8**. The operation of a computer system such as that shown in FIG. **8** is readily known in the art and is not discussed in detail in this application. Code to implement the present invention can be stored in computer-readable storage media such as one or more of system memory **817**, fixed disk **844**, optical disk **842**, or floppy disk **838**. The operating system provided on computer system **810** may be MS-DOS®, MS-WINDOWS®, OS/2®, UNIX®, Linux®, or another known operating system.

Moreover, regarding the signals described herein, those skilled in the art will recognize that a signal can be directly transmitted from a first block to a second block, or a signal can be modified (e.g., amplified, attenuated, delayed, latched, buffered, inverted, filtered, or otherwise modified) between the blocks. Although the signals of the above described embodiment are characterized as transmitted from one block to the next, other embodiments of the present invention may include modified signals in place of such directly transmitted signals as long as the informational and/or functional aspect of the signal is transmitted between blocks. To some extent, a signal input at a second block can be conceptualized as a second signal derived from a first signal output from a first block due to physical limitations of the circuitry involved (e.g., there will inevitably be some attenuation and delay). Therefore, as used herein, a second signal derived from a first signal includes the first signal or any modifications to the first signal, whether due to circuit limitations or due to passage through other circuit elements which do not change the informational and/or final functional aspect of the first signal.

Other Embodiments

The present invention is well adapted to attain the advantages mentioned as well as others inherent therein. While the present invention has been depicted, described, and is defined by reference to particular embodiments of the present invention, such references do not imply a limitation on the invention, and no such limitation is to be inferred. The invention is capable of considerable modification, alteration, and equivalents in form and function as will occur to those ordinarily skilled in the pertinent arts. The depicted and described embodiments are examples only, and are not exhaustive of the scope of the invention.

The foregoing describes embodiments including components contained within other components (e.g., the various elements shown as components of communications unit **210**). Such architectures are merely examples, and, in fact, many other architectures can be implemented which achieve the same functionality. In an abstract but still definite sense, any arrangement of components to achieve the same functionality is effectively "associated" such that the desired functionality is achieved. Hence, any two components herein combined to achieve a particular functionality can be seen as "associated with" each other such that the desired functionality is achieved, irrespective of architectures or intermediate components. Likewise, any two components so associated can also be viewed as being "operably connected" or "operably coupled" to each other to achieve the desired functionality.

The foregoing detailed description has set forth various examples of the present invention via the use of block diagrams, flow charts, and examples. It will be understood by those within the art that each block diagram component, flow chart step, operation and/or component illustrated by the use of examples can be implemented, individually and/or collectively, by a wide range of hardware, software, firmware, or any combination thereof.

The above description is intended to be illustrative of the invention and should not be taken to be limiting. Other embodiments within the scope of the present invention are possible. Those skilled in the art will readily implement the steps necessary to provide the structures and the methods disclosed herein, and will understand that the process parameters and sequence of steps are given by way of example only and can be varied to achieve the desired structure as well as modifications that are within the scope of the invention. Variations and modifications of the embodiments disclosed herein can be made based on the description set forth herein, without departing from the scope of the invention.

Consequently, the invention is intended to be limited only by the scope of the appended claims, giving full cognizance to equivalence in all respects.

Although the present invention has been described in connection with several embodiments, the invention is not intended to be limited to the specific forms set forth herein. On the contrary, it is intended to cover such alternatives, modifications, and equivalents as can be reasonably included within the scope of the invention as defined by the appended claims.

What is claimed is:

1. A method performed by a network node coupled to an alarm system communications unit via a network, the method comprising:

receiving, by the network node, a first set of data over the network from the alarm system communications unit, wherein

the first set of data comprises keypad bus information,

the keypad bus information corresponds to a signal on a keypad bus of an alarm system controller, and

the keypad bus of the alarm system controller provides communication between an alarm processor of the alarm system controller, a keypad processor, and the alarm system communications unit; and

performing, by the network node, a first pre-determined response to the keypad bus information in the first set of data.

2. The method of claim **1** further comprising:

receiving, by the network node, a second set of data over the network, wherein

the second set of data comprises alarm condition information, and

the alarm condition information corresponds to a signal from an alarm system controller telecommunications interface; and

performing, by the network node, a second pre-determined response to the alarm condition information in the second set of data.

3. The method of claim **2** further comprising:

determining, by the network node, whether the first or second set of data contain reportable information to provide to a monitoring station; and

transmitting, by the network node, a description corresponding to the reportable information to the monitoring station, if the first or second set of data contains reportable information.

4. The method of claim **1** further comprising:

storing, by the network node, a set of responses to keypad bus information, wherein

the keypad bus information comprises one of a plurality of events and conditions reported on the keypad bus of the alarm system controller, and

each response of the set of responses corresponds to an event or condition of the plurality of events and conditions; and

selecting, by the network node, the pre-determined response to the keypad bus information in the first set of data from the set of responses.

5. The method of claim **4** wherein the pre-determined response comprises:

providing a description corresponding to the information in the first set of data to a selected user.

6. The method of claim **4** further comprising:

providing, by the network node, a user interface configured to enable a user to enter response data; and

storing, by the network node, the response data as a response of the set of responses.

7. The method of claim **1** further comprising: transmitting, by the network node, control information to the alarm system communications unit, wherein the first pre-determined response comprises said transmitting, said transmitting is performed over a selected communication mode by the network node, and the control information comprises data usable to control the alarm system controller,

the alarm system communications unit is coupled to an alarm processor of the alarm system controller via a keypad bus, and

the keypad bus provides communication between the alarm processor of the alarm system controller, a keypad processor, and the alarm system communications unit.

8. The method of claim **7** further comprising:

transmitting, by the alarm systems communications unit, the received control information to the alarm system controller, wherein

said transmitting the received control information is performed using the keypad bus,

said transmitting the received control information is performed using a protocol that is the same as that used between the keypad processor and the alarm system controller.

9. The method of claim **8** further comprising:

interpreting the received control information, by the alarm systems communication unit, prior to said transmitting the received control information, wherein

said interpreting the received control information converts the received control information into the protocol.

10. The method of claim **8** wherein said transmitting the received control information is performed to emulate communication between the keypad processor and the alarm system controller.

11. The method of claim **7** wherein the control information comprises one of a command to arm the alarm system controller and a command to disarm the alarm system controller.

12. An apparatus comprising:

means for receiving a first set of data over a network from an alarm system communication unit, wherein

the first set of data comprises keypad bus information,

the keypad bus information corresponds to a signal on a keypad bus of an alarm system controller, and

the keypad bus of the alarm system controller provides communication between an alarm processor of the alarm system controller, a keypad processor, and the alarm system communication unit; and

means for performing a first pre-determined response to the keypad bus information in the first set of data.

13. The apparatus of claim **12** further comprising:

means for receiving a second set of data over the network, wherein

the second set of data comprises alarm condition information, and

the alarm condition information corresponds to a signal from an alarm system controller telecommunications interface; and

means for performing a second pre-determined response to the alarm condition information in the second set of data.

14. The apparatus of claim **13** further comprising:

means for determining whether the first or second set of data contain reportable information to provide to a monitoring station; and

means for transmitting a description corresponding to the reportable information to the monitoring station, if the first or second set of data contains reportable information.

15. The apparatus of claim **12** further comprising:

means for storing a set of responses to keypad bus information, wherein

the keypad bus information comprises one of a plurality of events and conditions reported on the alarm system controller keypad bus, and

each response of the set of responses corresponds to an event or condition of the plurality of events and conditions; and

means for selecting the pre-determined response to the keypad bus information in the first set of data from the set of responses.

16. The apparatus of claim **15** further comprising:

means for providing a user interface configured to enable a user to enter response data; and

means for storing the response data as a response of the set of responses.

* * * * *

EXHIBIT 3

US009141276B2

(12) **United States Patent**
Dawes et al.

(10) **Patent No.: US 9,141,276 B2**
(45) **Date of Patent: *Sep. 22, 2015**

(54) **INTEGRATED INTERFACE FOR MOBILE DEVICE**

(75) Inventors: **Paul J. Dawes**, Woodside, CA (US); **Jim Fulker**, Palo Alto, CA (US); **Carolyn Wales**, Menlo Park, CA (US); **Reza Raji**, Menlo Park, CA (US); **Gerald Gutt**, Tucson, AZ (US)

(73) Assignee: **iControl Networks, Inc.**, Redwood City, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 510 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/311,365**

(22) Filed: **Dec. 5, 2011**

(65) **Prior Publication Data**

US 2012/0260184 A1 Oct. 11, 2012

Related U.S. Application Data

(63) Continuation of application No. 12/197,895, filed on Aug. 25, 2008, now Pat. No. 8,073,931, and a continuation-in-part of application No. 11/084,232, filed on Mar. 16, 2005, now Pat. No. 8,335,842, and a

(Continued)

(51) **Int. Cl.**

G06F 15/16	(2006.01)
G06F 3/0488	(2013.01)
G08B 25/00	(2006.01)
G08B 25/14	(2006.01)
G06F 17/30	(2006.01)

(52) **U.S. Cl.**
CPC ***G06F 3/0488*** (2013.01); ***G08B 25/008*** (2013.01); ***G08B 25/14*** (2013.01); *G06F 17/30873* (2013.01)

(58) **Field of Classification Search**
CPC G06F 3/0488; G06F 17/30873
USPC 709/202, 203, 219, 223, 224; 715/716, 715/736
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

8,046,411 B2 * 10/2011 Hayashi et al. 709/204

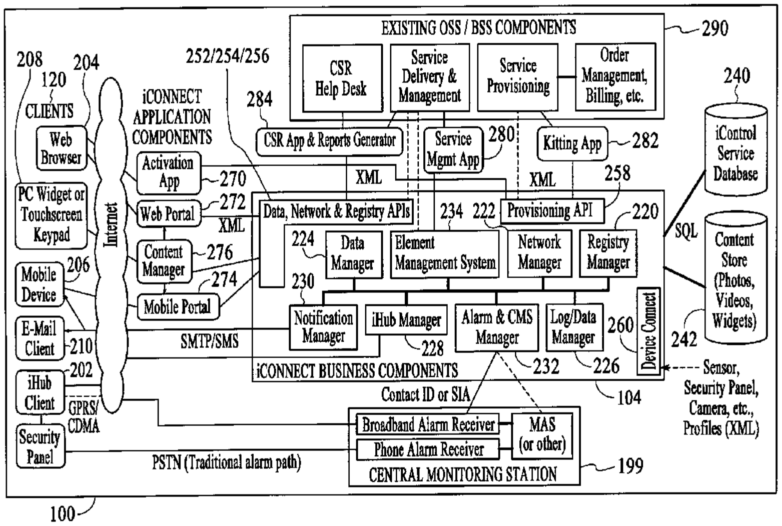
(Continued)

Primary Examiner — Krisna Lim
(74) *Attorney, Agent, or Firm* — IPR Law Group, PC

(57) **ABSTRACT**

An integrated security system integrates broadband and mobile access and control with conventional security systems and premise devices to provide a tri-mode security network that with remote connectivity and access. The integrated security system includes a touchscreen providing security keypad functionality as well as content management and presentation, and is used as a security system interface and an interface for interacting with a network. The integrated security system delivers remote premise monitoring and control functionality to conventional monitored premise protection and complements existing premise protection equipment. The integrated security system integrates into the premise network and couples wirelessly with the conventional security panel, enabling broadband access to premise security systems. Automation devices can be added, enabling users to remotely see live video or pictures and control home devices via a personal web portal, mobile phone, or other client device. Users can receive notifications of detected events via electronic message.

18 Claims, 18 Drawing Sheets


EXISTING OSS / BSS COMPONENTS
290
CSR Help Desk
Service Delivery & Management
Service Provisioning
Order Management, Billing, etc.
208
204
120
CLIENTS
Web Browser
PC Widget or Touchscreen Keypad
Mobile Device
206
E-Mail Client
210
202
iHub Client
Security Panel
GPRS/CDMA
Internet
252/254/256
iCONNECT APPLICATION COMPONENTS
284
CSR App & Reports Generator
Service Mgmt App
280
Kitting App
282
Activation App
270
Web Portal
272
XML
Content Manager
276
274
Mobile Portal
Data, Network & Registry APIs
234
222
Provisioning API
220
258
224
Data Manager
Element Management System
Network Manager
Registry Manager
230
Notification Manager
iHub Manager
228
Alarm & CMS Manager
Log/Data Manager
260
Device Connect
232
226
SMTP/SMS
iCONNECT BUSINESS COMPONENTS
104
Contact ID or SIA
Broadband Alarm Receiver
Phone Alarm Receiver
MAS (or other)
PSTN (Traditional alarm path)
CENTRAL MONITORING STATION
199
240
iControl Service Database
SQL
Content Store (Photos, Videos, Widgets)
242
Sensor, Security Panel, Camera, etc., Profiles (XML)
100

Related U.S. Application Data

continuation-in-part of application No. 11/761,718, filed on Jun. 12, 2007, now Pat. No. 7,711,796, and a continuation-in-part of application No. 11/761,745, filed on Jun. 12, 2007, now Pat. No. 8,635,350, and a continuation-in-part of application No. 12/019,554, filed on Jan. 24, 2008, now Pat. No. 7,911,341, and a continuation-in-part of application No. 12/019,568, filed on Jan. 24, 2008, and a continuation-in-part of application No. 12/189,757, filed on Aug. 11, 2008, now Pat. No. 8,473,619.

(56) **References Cited**

U.S. PATENT DOCUMENTS

8,073,931	B2 *	12/2011	Dawes et al.	709/219
8,311,526	B2 *	11/2012	Forstall et al.	455/414.3
8,499,038	B1 *	7/2013	Vucurevich	709/204
2006/0271695	A1 *	11/2006	Lavian	709/229
2007/0245223	A1 *	10/2007	Siedzik et al.	715/500.1
2008/0168404	A1 *	7/2008	Ording	715/863
2010/0298024	A1 *	11/2010	Choi	455/550.1

* cited by examiner

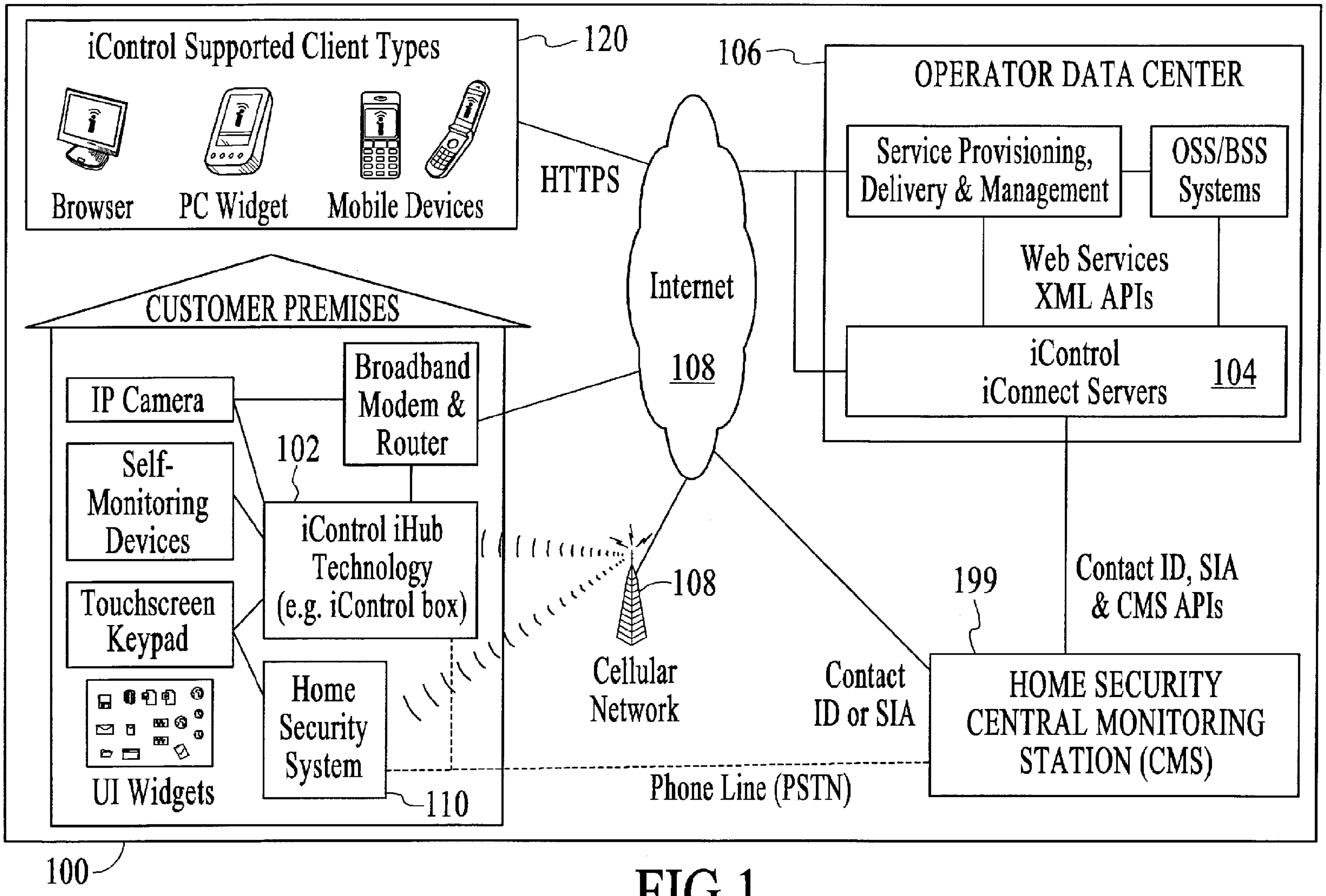

iControl Supported Client Types
120
Browser
PC Widget
Mobile Devices
HTTPS
106
OPERATOR DATA CENTER
Service Provisioning, Delivery & Management
OSS/BSS Systems
Web Services XML APIs
iControl iConnect Servers
104
Internet
108
CUSTOMER PREMISES
IP Camera
Broadband Modem & Router
102
Self-Monitoring Devices
iControl iHub Technology (e.g. iControl box)
Touchscreen Keypad
Home Security System
110
UI Widgets
108
Cellular Network
Contact ID or SIA
199
Contact ID, SIA & CMS APIs
HOME SECURITY CENTRAL MONITORING STATION (CMS)
Phone Line (PSTN)
100

FIG.1

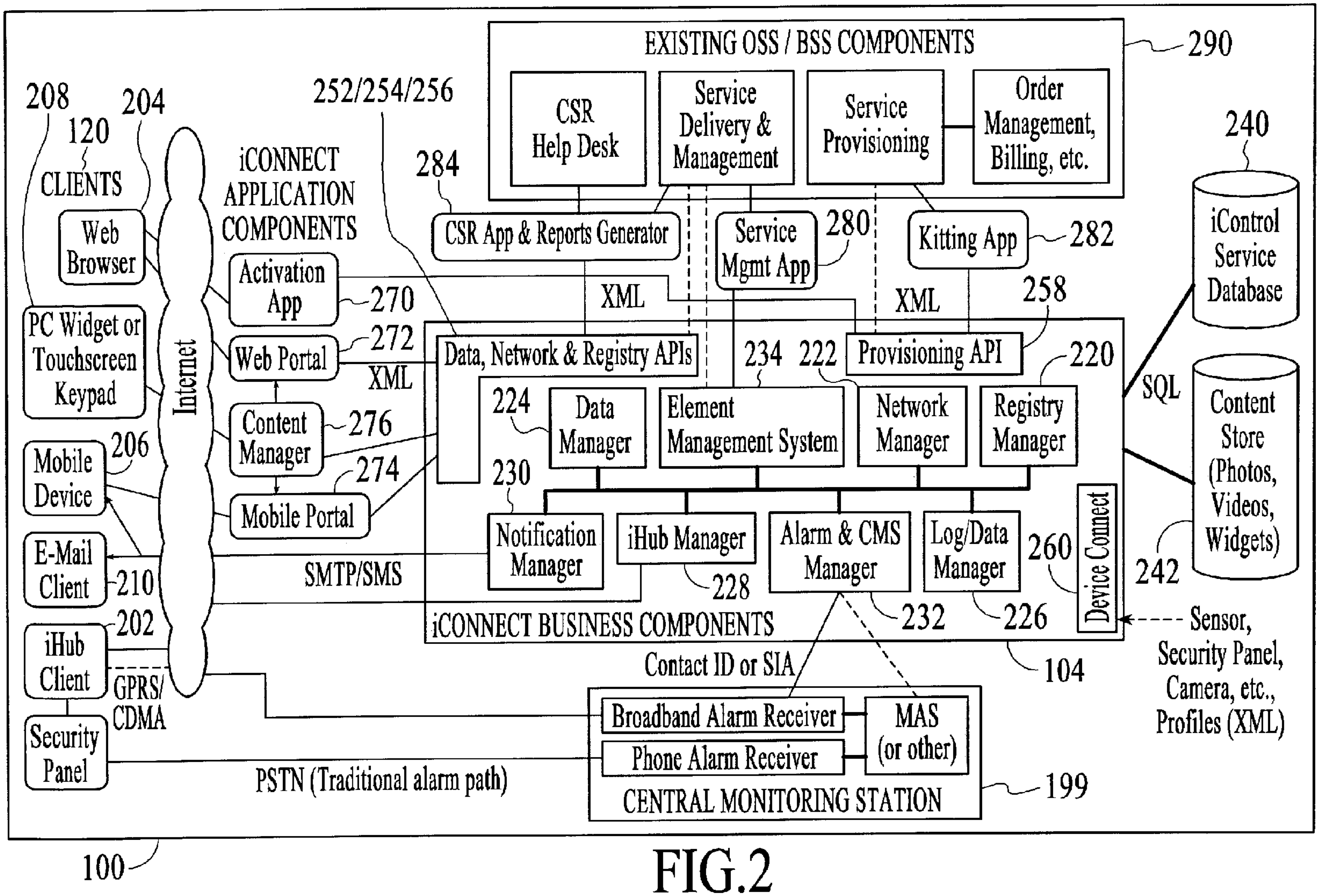

EXISTING OSS / BSS COMPONENTS
290
CSR Help Desk
Service Delivery & Management
Service Provisioning
Order Management, Billing, etc.
208
204
120
CLIENTS
Web Browser
PC Widget or Touchscreen Keypad
Mobile Device
206
E-Mail Client
210
iHub Client
202
GPRS/ CDMA
Security Panel
Internet
iCONNECT APPLICATION COMPONENTS
252/254/256
284
Activation App
270
Web Portal
272
XML
Content Manager
276
Mobile Portal
274
CSR App & Reports Generator
Service Mgmt App
280
Kitting App
282
XML
XML
258
240
iControl Service Database
Data, Network & Registry APIs
234
222
Provisioning API
220
224
Data Manager
Element Management System
Network Manager
Registry Manager
SQL
Content Store (Photos, Videos, Widgets)
230
Notification Manager
iHub Manager
228
Alarm & CMS Manager
232
Log/Data Manager
226
260
Device Connect
242
SMTP/SMS
iCONNECT BUSINESS COMPONENTS
104
Sensor, Security Panel, Camera, etc., Profiles (XML)
Contact ID or SIA
Broadband Alarm Receiver
Phone Alarm Receiver
MAS (or other)
PSTN (Traditional alarm path)
CENTRAL MONITORING STATION
199
100

FIG.2

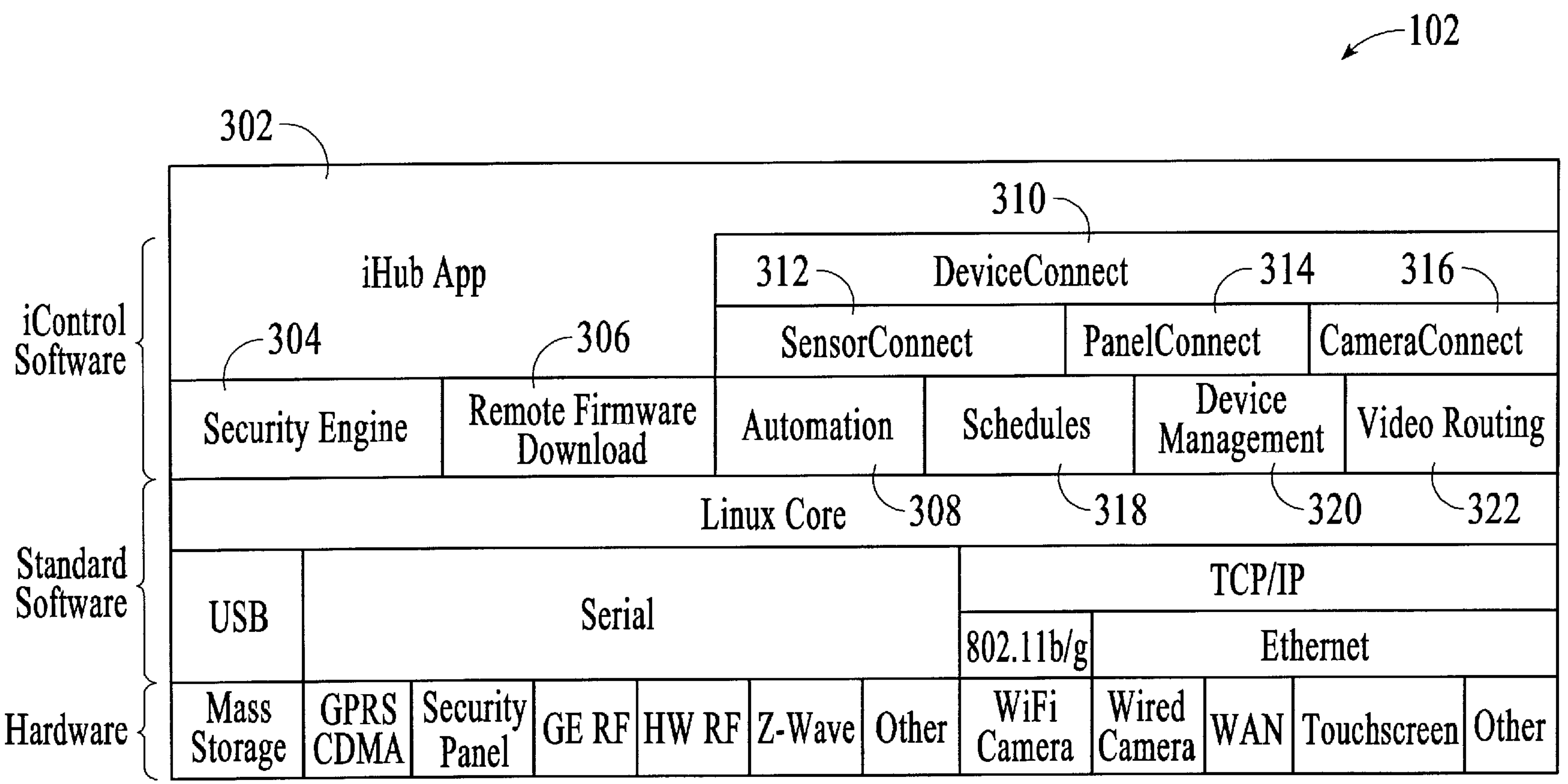

102
302
310
iHub App
312
DeviceConnect
314
316
iControl Software
304
306
SensorConnect
PanelConnect
CameraConnect
Security Engine
Remote Firmware Download
Automation
Schedules
Device Management
Video Routing
Linux Core
308
318
320
322
Standard Software
USB
Serial
TCP/IP
802.11b/g
Ethernet
Hardware
Mass Storage
GPRS CDMA
Security Panel
GE RF
HW RF
Z-Wave
Other
WiFi Camera
Wired Camera
WAN
Touchscreen
Other

FIG.3

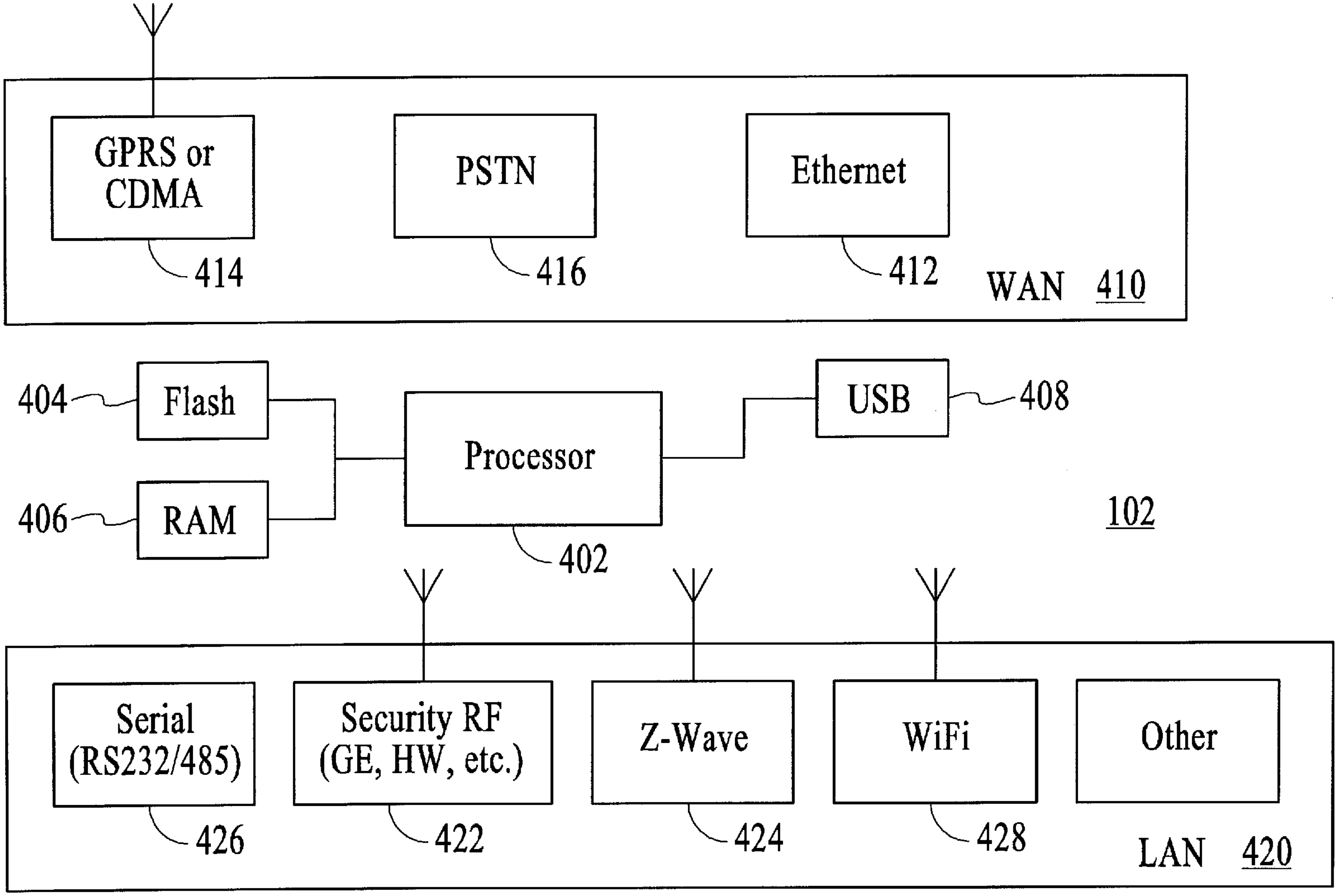

GPRS or CDMA
414
PSTN
416
Ethernet
412
WAN 410
404
Flash
406
RAM
Processor
402
USB
408
102
Serial (RS232/485)
426
Security RF (GE, HW, etc.)
422
Z-Wave
424
WiFi
428
Other
LAN 420

FIG.4

FIG.5

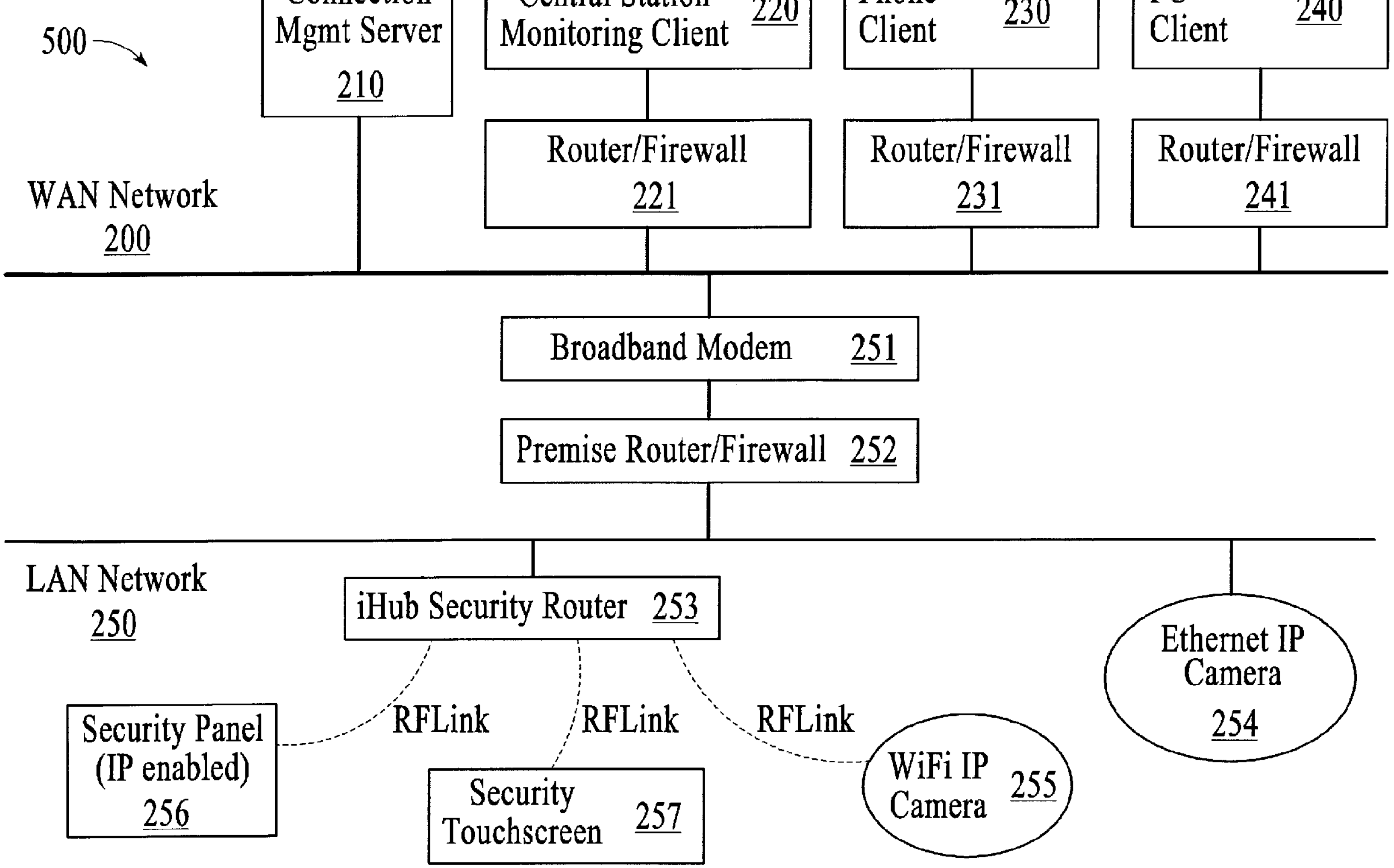
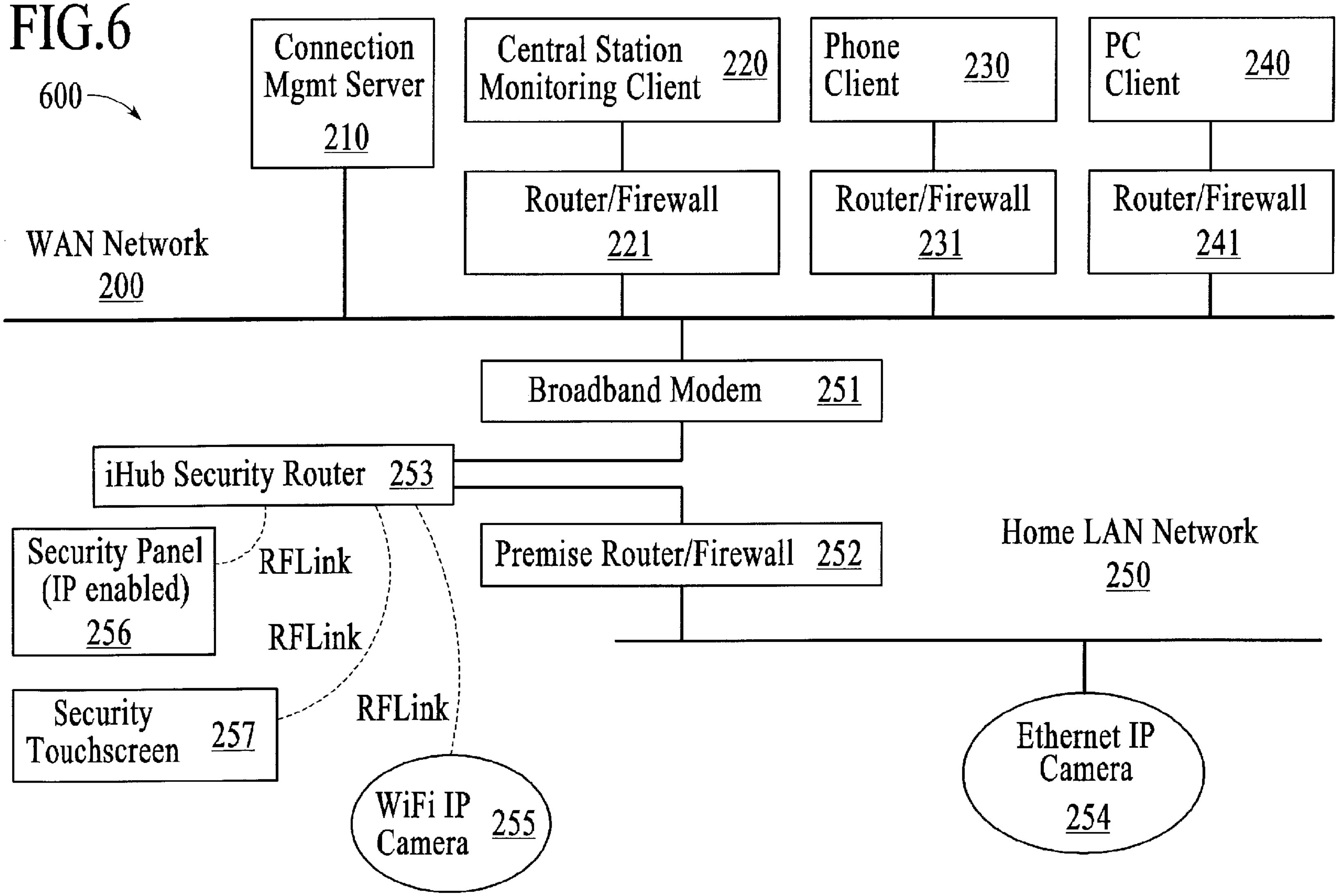

500
Connection Mgmt Server 210
Central Station Monitoring Client 220
Phone Client 230
PC Client 240
Router/Firewall 221
Router/Firewall 231
Router/Firewall 241
WAN Network 200
Broadband Modem 251
Premise Router/Firewall 252
LAN Network 250
iHub Security Router 253
Ethernet IP Camera 254
RFLink
RFLink
RFLink
Security Panel (IP enabled) 256
Security Touchscreen 257
WiFi IP Camera 255

FIG.6


600
Connection Mgmt Server 210
Central Station Monitoring Client 220
Phone Client 230
PC Client 240
Router/Firewall 221
Router/Firewall 231
Router/Firewall 241
WAN Network 200
Broadband Modem 251
iHub Security Router 253
Premise Router/Firewall 252
Home LAN Network 250
Security Panel (IP enabled) 256
RFLink
RFLink
RFLink
Security Touchscreen 257
WiFi IP Camera 255
Ethernet IP Camera 254

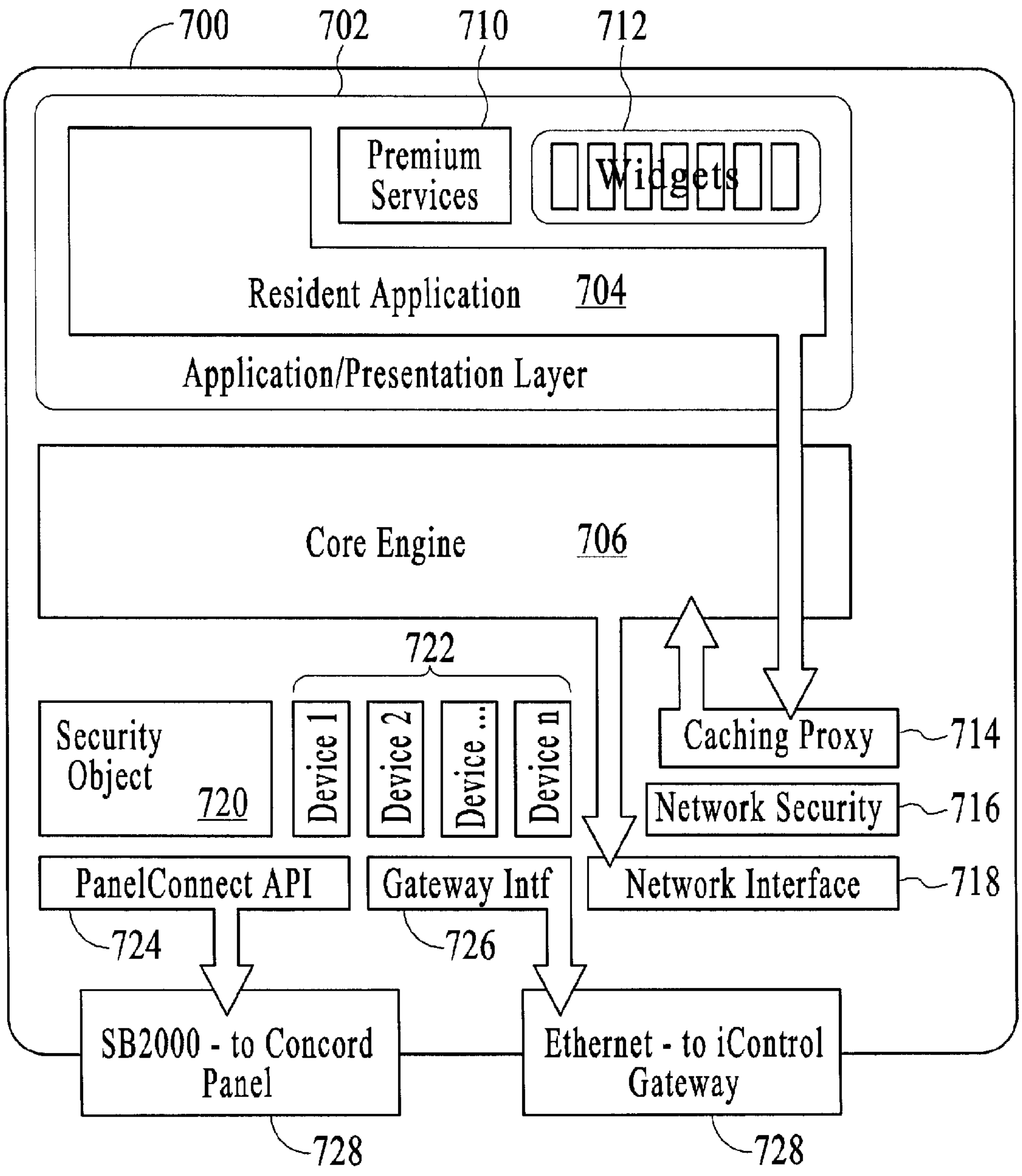
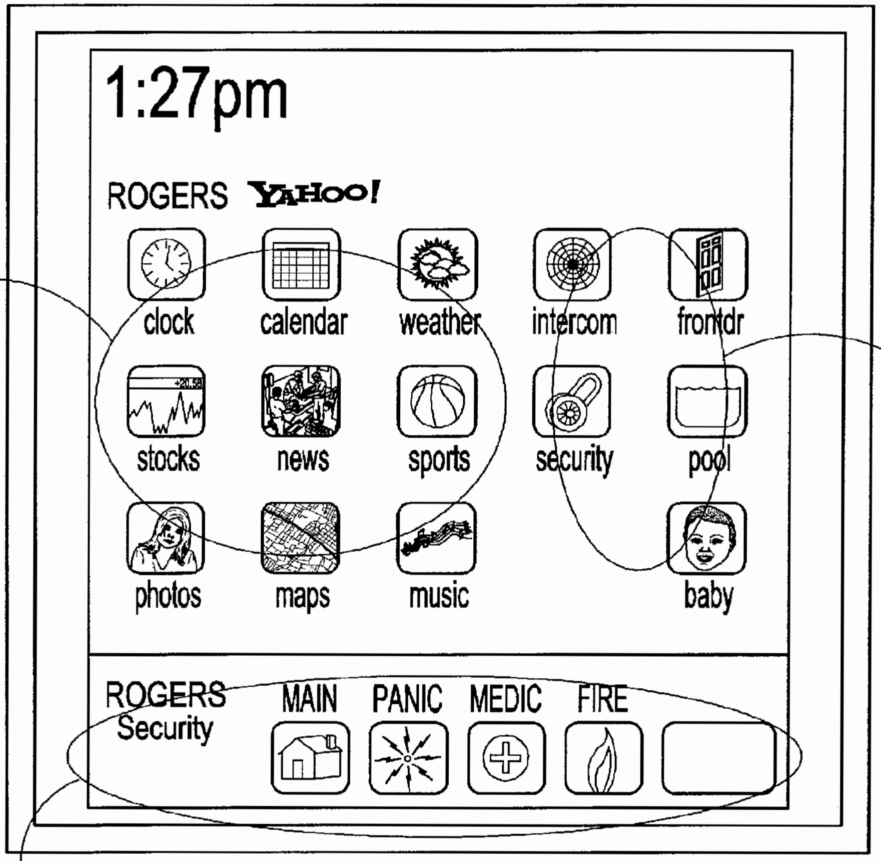

700
702
710
712
Premium Services
Widgets
Resident Application 704
Application/Presentation Layer
Core Engine 706
722
Security Object 720
Device 1
Device 2
Device ...
Device n
Caching Proxy
714
Network Security
716
PanelConnect API
Gateway Intf
Network Interface
718
724
726
SB2000 - to Concord Panel
Ethernet - to iControl Gateway
728
728

FIG.7

800

804
Widget Manager UI-
Displays available
widgets


1:27pm
ROGERS YAHOO!
clock
calendar
weather
intercom
frontdr
stocks
news
sports
security
pool
photos
maps
music
baby
ROGERS
Security
MAIN
PANIC
MEDIC
FIRE

806
Service Manager UI-
Displays additional
services available

802
Resident application UI-
Core security functionality,
always available

FIG.8

FIG.9

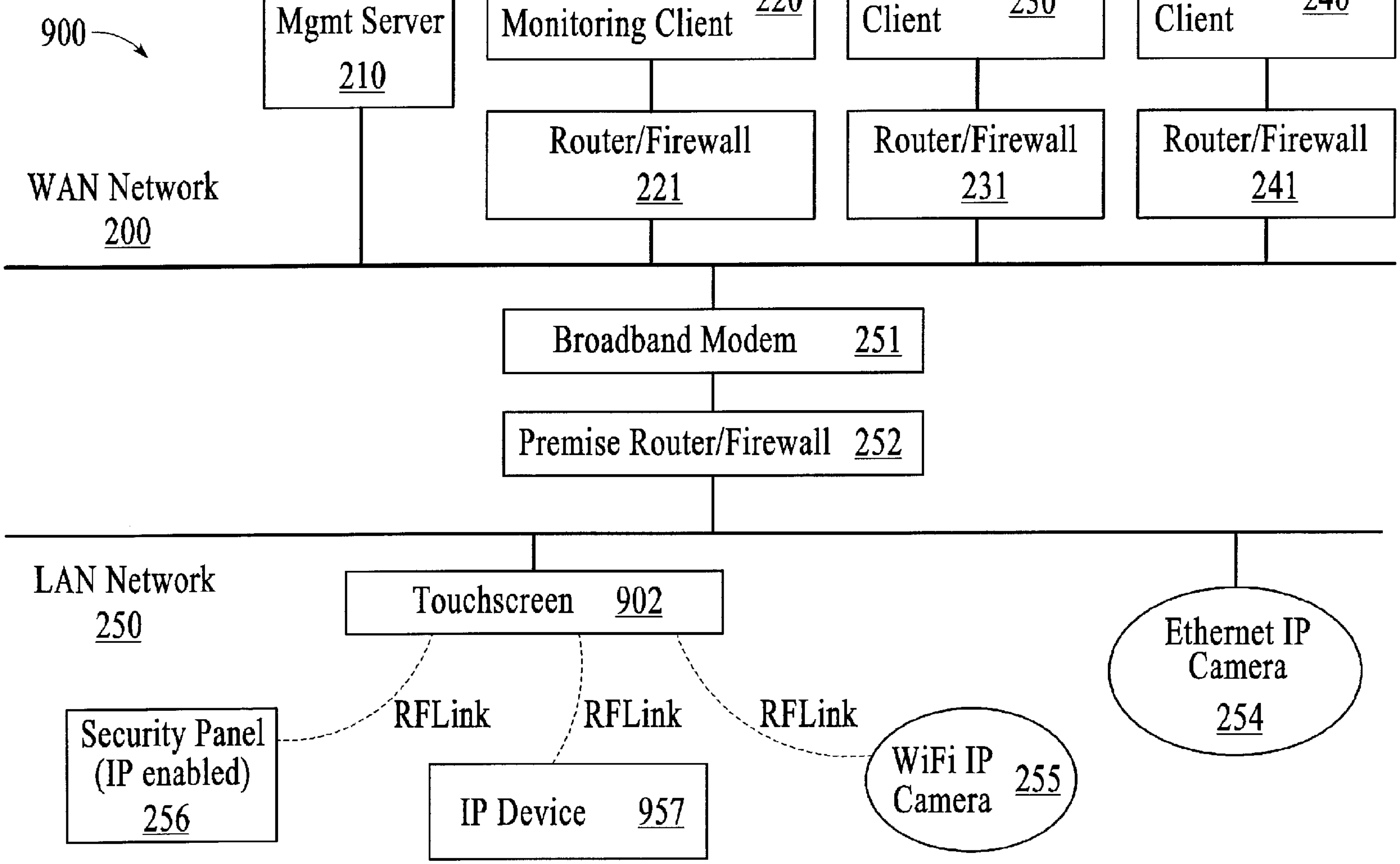
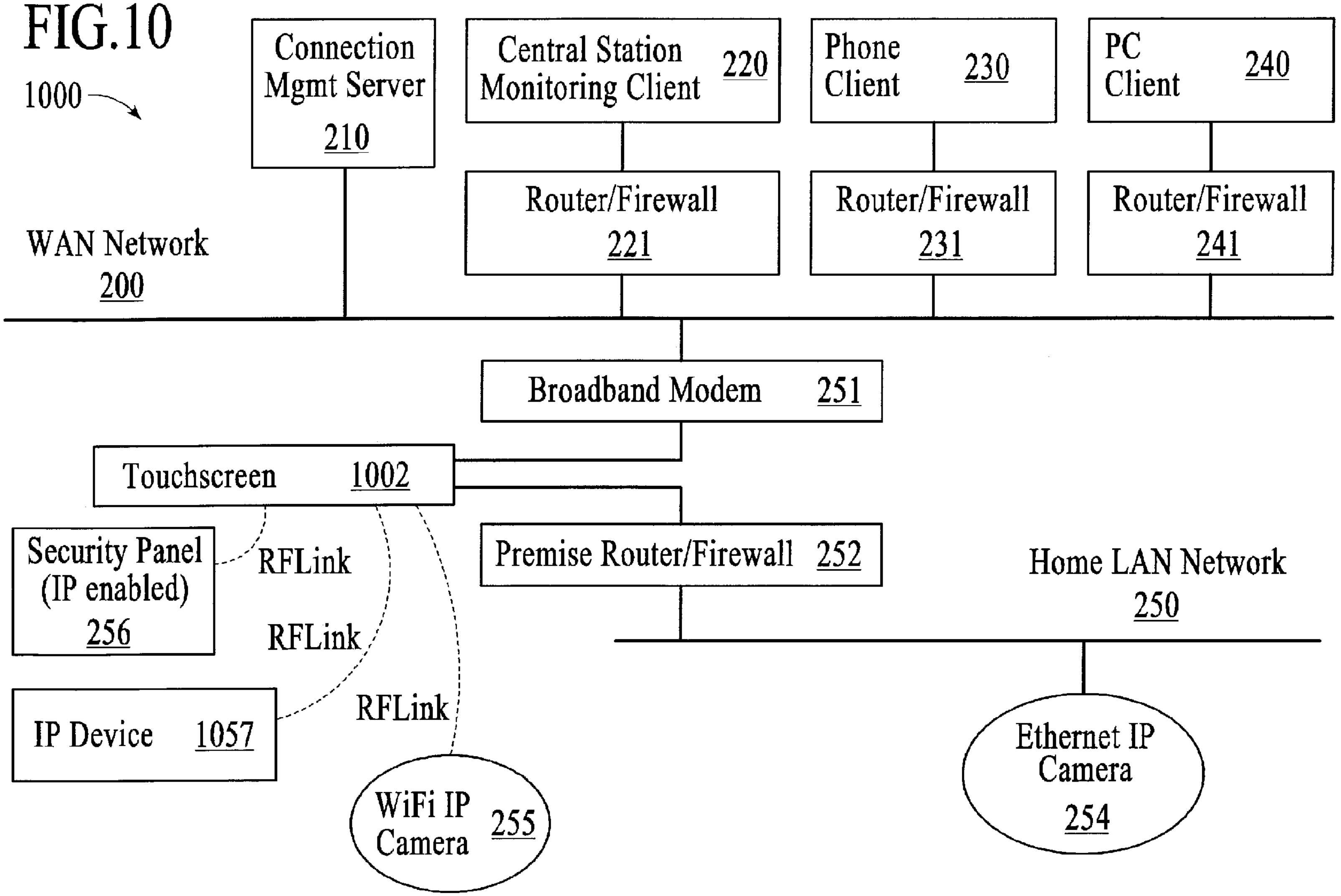

900
Connection Mgmt Server 210
Central Station Monitoring Client 220
Phone Client 230
PC Client 240
Router/Firewall 221
Router/Firewall 231
Router/Firewall 241
WAN Network 200
Broadband Modem 251
Premise Router/Firewall 252
LAN Network 250
Touchscreen 902
Ethernet IP Camera 254
RFLink
RFLink
RFLink
Security Panel (IP enabled) 256
IP Device 957
WiFi IP Camera 255

FIG.10


1000
Connection Mgmt Server 210
Central Station Monitoring Client 220
Phone Client 230
PC Client 240
Router/Firewall 221
Router/Firewall 231
Router/Firewall 241
WAN Network 200
Broadband Modem 251
Touchscreen 1002
Premise Router/Firewall 252
Security Panel (IP enabled) 256
RFLink
RFLink
RFLink
Home LAN Network 250
IP Device 1057
WiFi IP Camera 255
Ethernet IP Camera 254

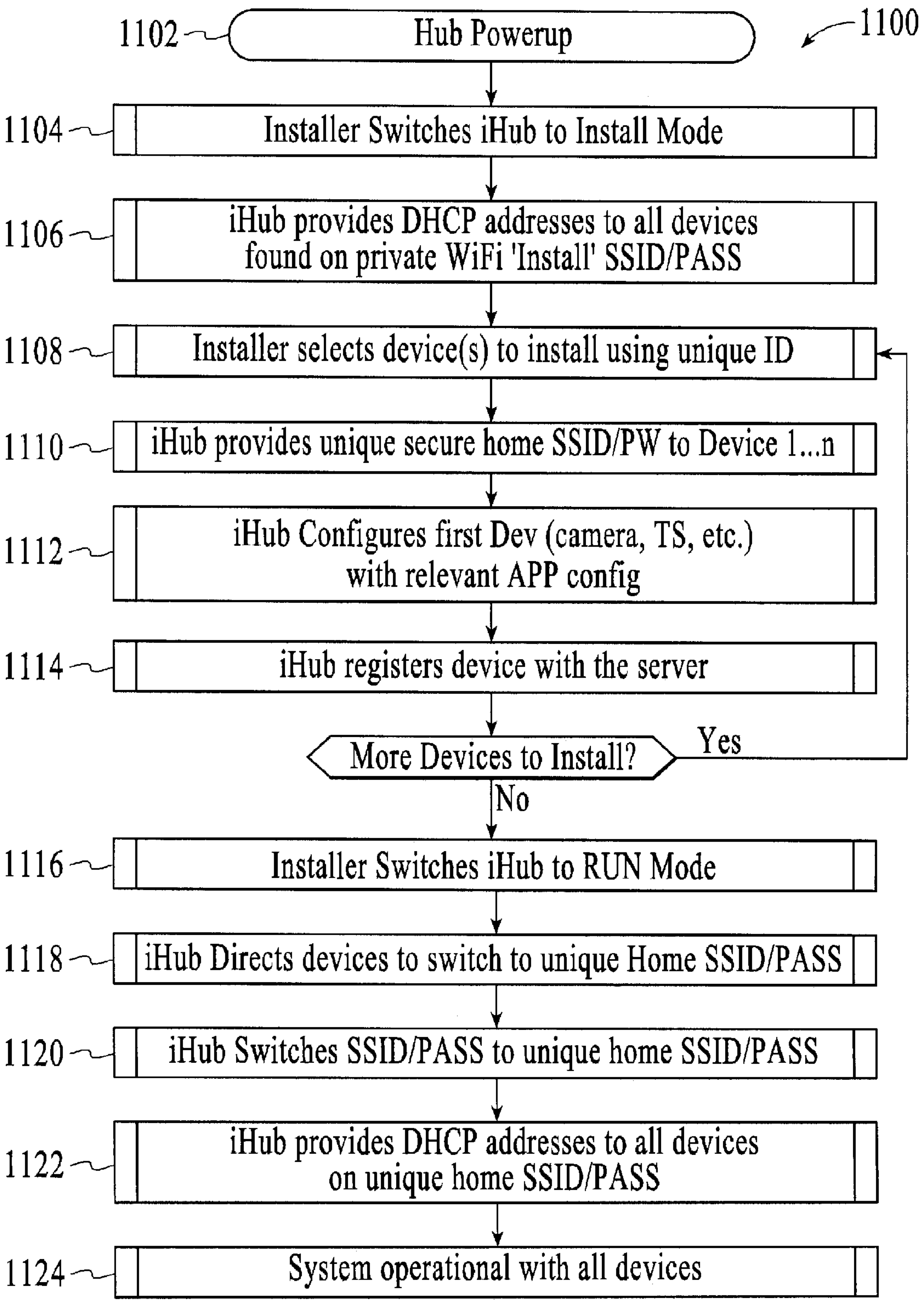

1100
1102
Hub Powerup
1104
Installer Switches iHub to Install Mode
1106
iHub provides DHCP addresses to all devices found on private WiFi 'Install' SSID/PASS
1108
Installer selects device(s) to install using unique ID
1110
iHub provides unique secure home SSID/PW to Device 1...n
1112
iHub Configures first Dev (camera, TS, etc.) with relevant APP config
1114
iHub registers device with the server
More Devices to Install?
Yes
No
1116
Installer Switches iHub to RUN Mode
1118
iHub Directs devices to switch to unique Home SSID/PASS
1120
iHub Switches SSID/PASS to unique home SSID/PASS
1122
iHub provides DHCP addresses to all devices on unique home SSID/PASS
1124
System operational with all devices

FIG.11

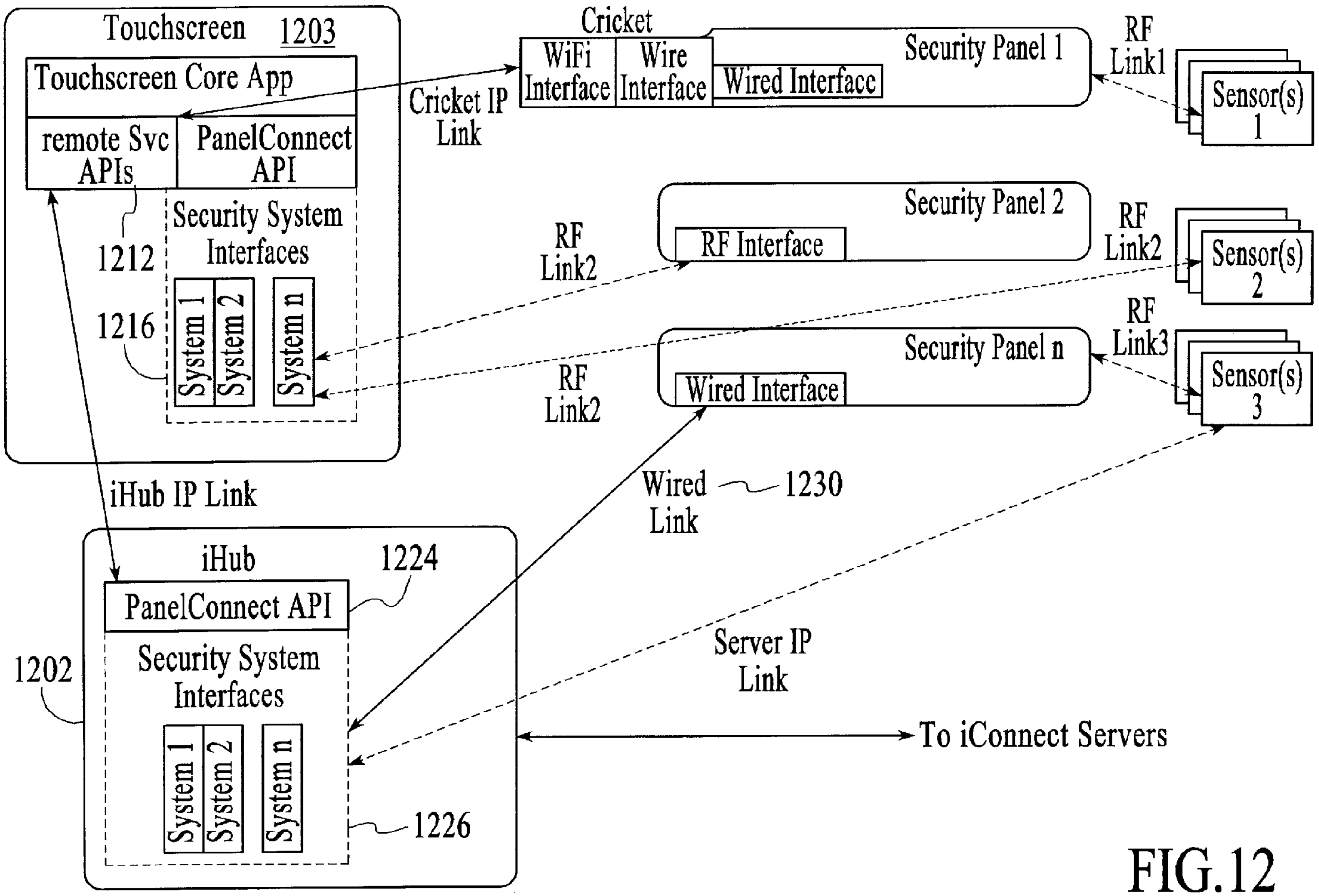

Touchscreen
1203
Touchscreen Core App
remote Svc APIs
PanelConnect API
1212
Security System Interfaces
1216
System 1
System 2
System n
Cricket
WiFi Interface
Wire Interface
Wired Interface
Security Panel 1
Cricket IP Link
RF Link1
Sensor(s) 1
Security Panel 2
RF Interface
RF Link2
RF Link2
Sensor(s) 2
Security Panel n
Wired Interface
RF Link3
RF Link2
Sensor(s) 3
iHub IP Link
Wired Link
1230
iHub
1224
PanelConnect API
1202
Security System Interfaces
System 1
System 2
System n
1226
Server IP Link
To iConnect Servers

FIG.12

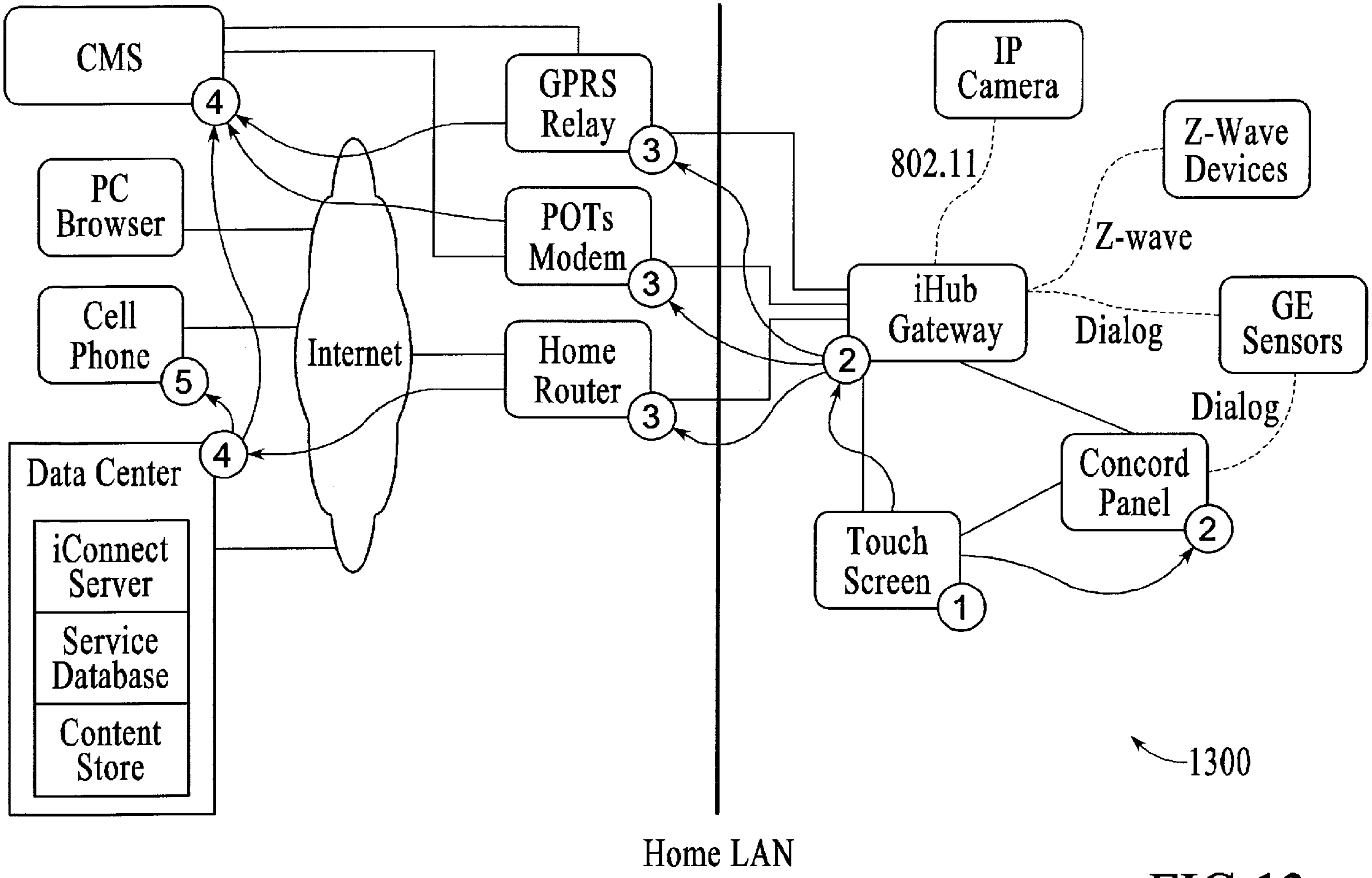

CMS
4
PC Browser
Cell Phone
5
Data Center
4
iConnect Server
Service Database
Content Store
Internet
GPRS Relay
3
POTs Modem
3
Home Router
3
Home LAN
IP Camera
802.11
Z-Wave Devices
Z-wave
iHub Gateway
2
Dialog
GE Sensors
Dialog
Concord Panel
2
Touch Screen
1
1300

FIG.13

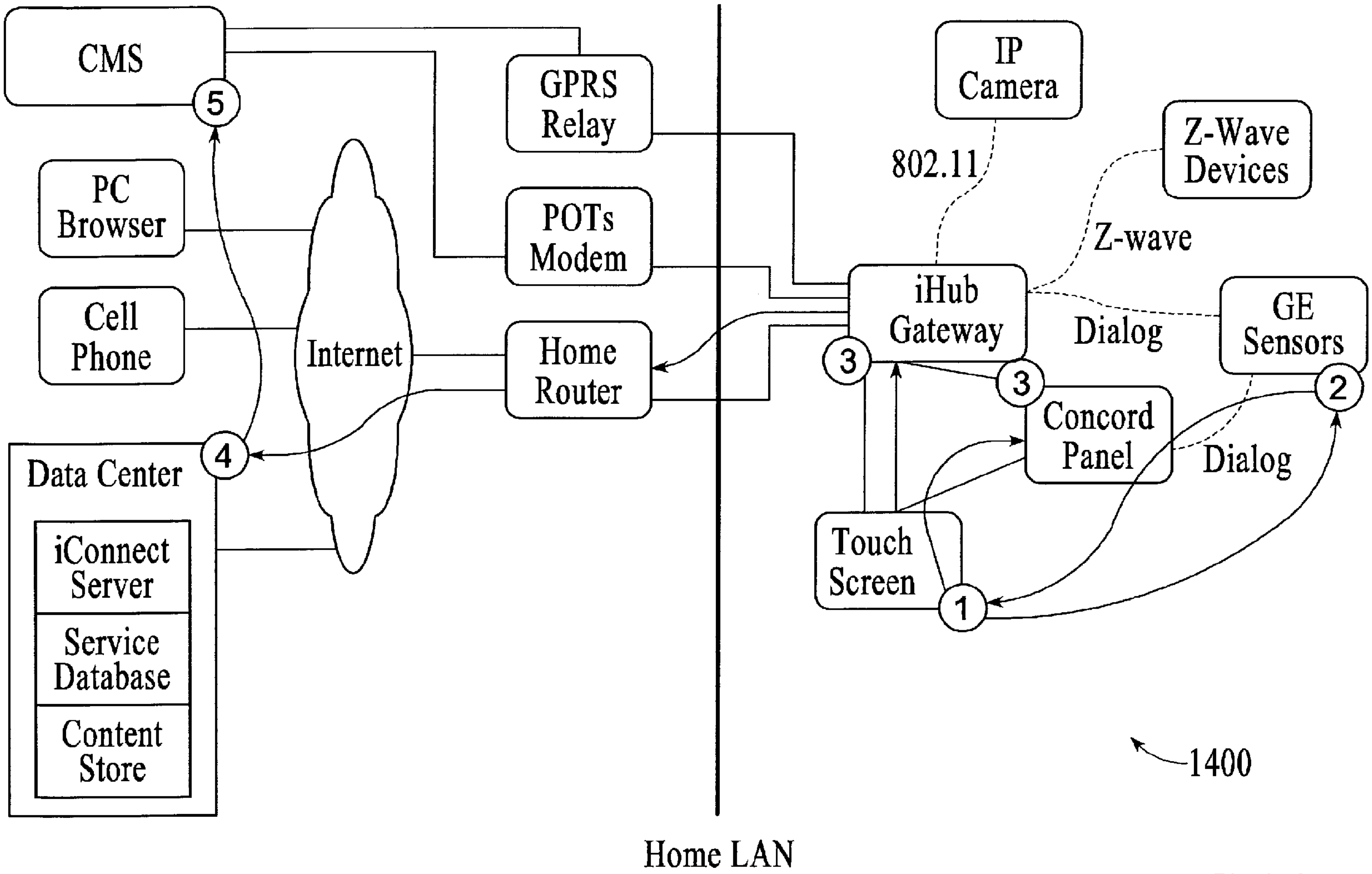

CMS
5
PC
Browser
Cell
Phone
Data Center
4
iConnect
Server
Service
Database
Content
Store
Internet
GPRS
Relay
POTs
Modem
Home
Router
Home LAN
IP
Camera
802.11
Z-Wave
Devices
Z-wave
iHub
Gateway
Dialog
GE
Sensors
3
3
2
Concord
Panel
Dialog
Touch
Screen
1
1400

FIG.14

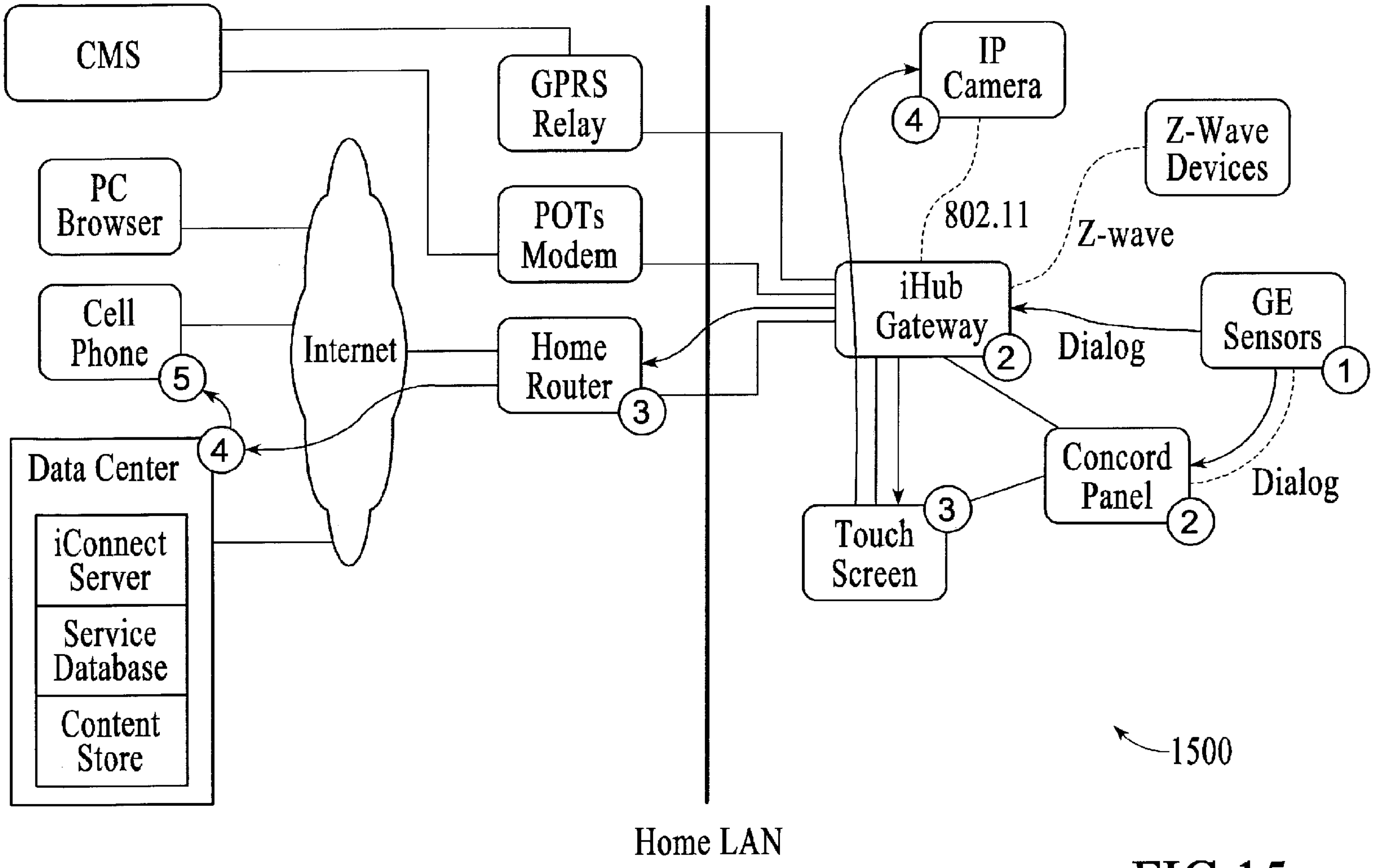

CMS
GPRS Relay
POTs Modem
PC Browser
Cell Phone
5
Internet
Home Router
3
Data Center
4
iConnect Server
Service Database
Content Store
Home LAN
IP Camera
4
802.11
Z-Wave Devices
Z-wave
iHub Gateway
2
Dialog
GE Sensors
1
Concord Panel
2
Dialog
Touch Screen
3
1500

FIG.15

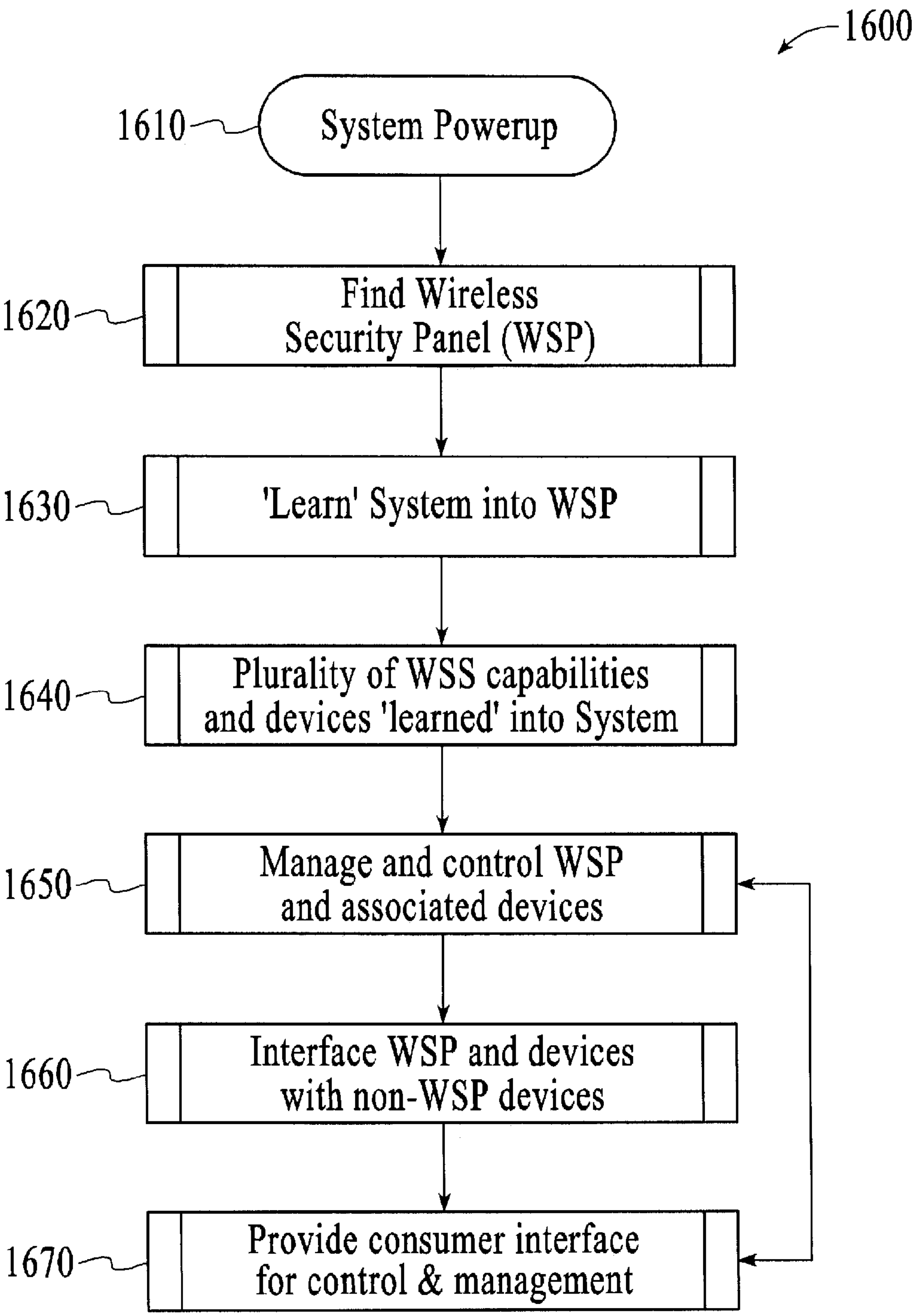

1600
1610
System Powerup
1620
Find Wireless
Security Panel (WSP)
1630
'Learn' System into WSP
1640
Plurality of WSS capabilities
and devices 'learned' into System
1650
Manage and control WSP
and associated devices
1660
Interface WSP and devices
with non-WSP devices
1670
Provide consumer interface
for control & management

FIG.16

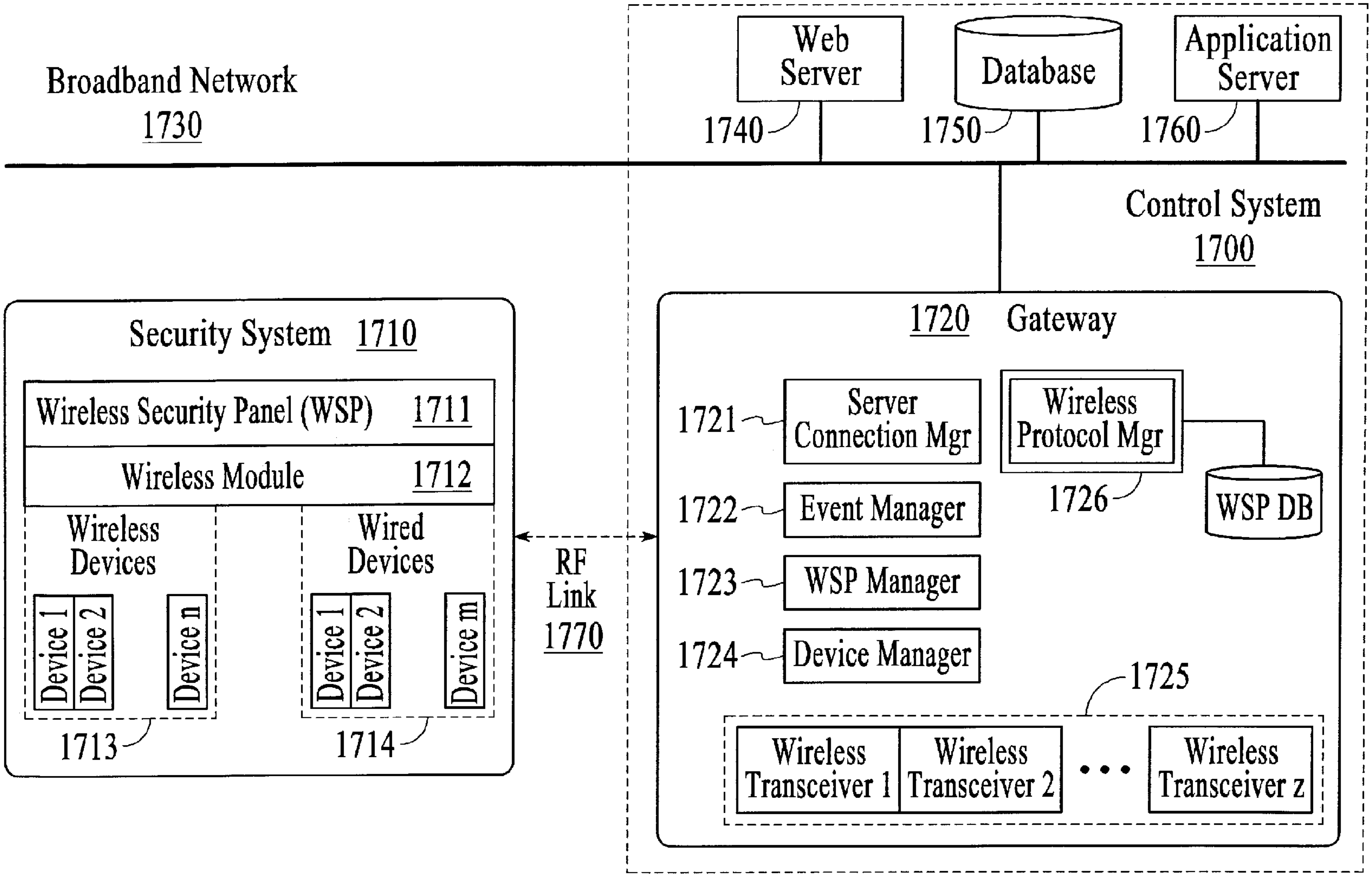

Broadband Network
1730
Web Server
1740
Database
1750
Application Server
1760
Control System
1700
Security System 1710
Wireless Security Panel (WSP) 1711
Wireless Module 1712
Wireless Devices
Device 1
Device 2
Device n
1713
Wired Devices
Device 1
Device 2
Device m
1714
RF Link
1770
1720 Gateway
1721
Server Connection Mgr
1722
Event Manager
1723
WSP Manager
1724
Device Manager
Wireless Protocol Mgr
1726
WSP DB
1725
Wireless Transceiver 1
Wireless Transceiver 2
Wireless Transceiver z

FIG.17

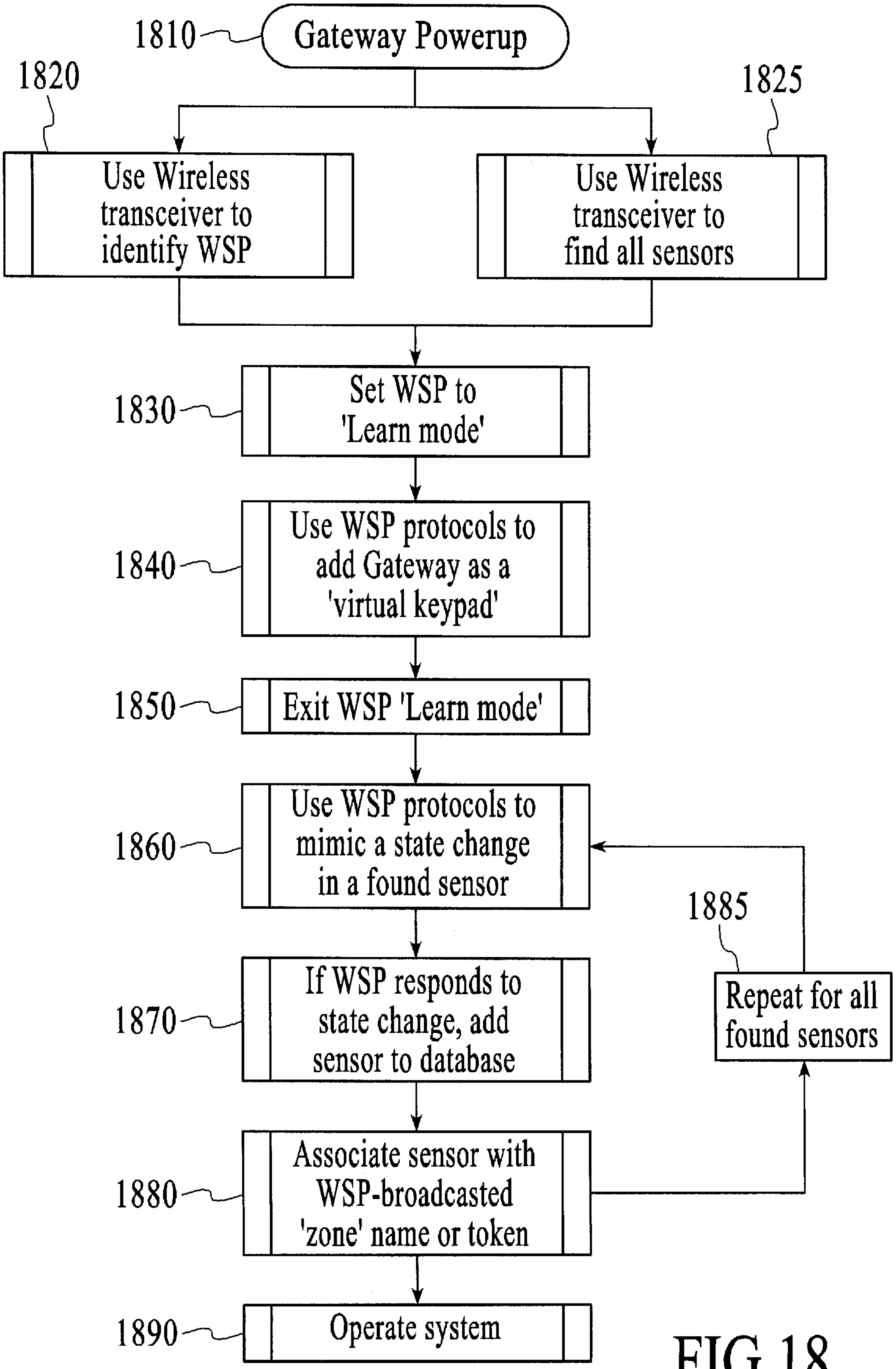

1810
Gateway Powerup
1820
Use Wireless transceiver to identify WSP
1825
Use Wireless transceiver to find all sensors
1830
Set WSP to 'Learn mode'
1840
Use WSP protocols to add Gateway as a 'virtual keypad'
1850
Exit WSP 'Learn mode'
1860
Use WSP protocols to mimic a state change in a found sensor
1885
Repeat for all found sensors
1870
If WSP responds to state change, add sensor to database
1880
Associate sensor with WSP-broadcasted 'zone' name or token
1890
Operate system

FIG.18

INTEGRATED INTERFACE FOR MOBILE DEVICE

RELATED APPLICATIONS

This application is a continuation of U.S. patent application Ser. No. 12/197,895, filed Aug. 25, 2008, now U.S. Pat. No. 8,073,931.

This application is a continuation in part application of U.S. patent application Ser. No. 11/084,232, filed Mar. 16, 2005, now U.S. Pat. No. 8,335,842.

This application is a continuation in part application of U.S. patent application Ser. No. 11/761,718, filed Jun. 12, 2007, now US Pat. No. 7,711,796.

This application is a continuation in part application of U.S. patent application Ser. No. 11/761,745, filed. Jun. 12, 2007.

This application is a continuation in part application of U.S. patent application Ser. No. 12/019,554, filed Jan. 24, 2008, now U.S. Pat. No. 7,911,341.

This application is a continuation in part application of U.S. patent application Ser. No. 12/019,568, filed Jan. 24, 2008.

This application is a continuation in part application of U.S. patent application Ser. No. 12/189,757, filed Aug. 11, 2008, now U.S Pat. No. 8,473,619.

TECHNICAL FIELD

The embodiments described herein relate generally to a method and apparatus for improving the capabilities of security systems in home and business applications. More particularly, the embodiments described herein relate to a touchscreen device that integrates security system control and functionality with network content interactivity, management and presentation.

BACKGROUND

The field of home and small business security is dominated by technology suppliers who build comprehensive 'closed' security systems, where the individual components (sensors, security panels, keypads) operate solely within the confines of a single vendor solution. For example, a wireless motion sensor from vendor A cannot be used with a security panel from vendor B. Each vendor typically has developed sophisticated proprietary wireless technologies to enable the installation and management of wireless sensors, with little or no ability for the wireless devices to operate separate from the vendor's homogeneous system. Furthermore, these traditional systems are extremely limited in their ability to interface either to a local or wide area standards-based network (such as an IP network); most installed systems support only a low-bandwidth, intermittent connection utilizing phone lines or cellular (RF) backup systems. Wireless security technology from providers such as GE Security, Honeywell, and DSC/Tyco are well known in the art, and are examples of this proprietary approach to security systems for home and business.

Furthermore, with the proliferation of the internet, ethernet and WiFi local area networks (LANs) and advanced wide area networks (WANs) that offer high bandwidth, low latency connections (broadband), as well as more advanced wireless WAN data networks (e.g. GPRS or CDMA 1xRTT) there increasingly exists the networking capability to extend these traditional security systems to offer enhanced functionality. In addition, the proliferation of broadband access has driven

a corresponding increase in home and small business networking technologies and devices. It is desirable to extend traditional security systems to encompass enhanced functionality such as the ability to control and manage security systems from the world wide web, cellular telephones, or advanced function internet-based devices. Other desired functionality includes an open systems approach to interface home security systems to home and small business networks.

Due to the proprietary approach described above, the traditional vendors are the only ones capable of taking advantage of these new network functions. To date, even though the vast majority of home and business customers have broadband network access in their premises, most security systems do not offer the advanced capabilities associated with high speed, low-latency LANs and WANs. This is primarily because the proprietary vendors have not been able to deliver such technology efficiently or effectively. Solution providers attempting to address this need are becoming known in the art, including three categories of vendors: traditional proprietary hardware providers such as Honeywell and GE Security; third party hard-wired module providers such as Alarm.com, NextAlarm, and uControl; and new proprietary systems providers such as InGrid.

A disadvantage of the prior art technologies of the traditional proprietary hardware providers arises due to the continued proprietary approach of these vendors. As they develop technology in this area it once again operates only with the hardware from that specific vendor, ignoring the need for a heterogeneous, cross-vendor solution. Yet another disadvantage of the prior art technologies of the traditional proprietary hardware providers arises due to the lack of experience and capability of these companies in creating open internet and web based solutions, and consumer friendly interfaces.

A disadvantage of the prior art technologies of the third party hard-wired module providers arises due to the installation and operational complexities and functional limitations associated with hardwiring a new component into existing security systems. Moreover, a disadvantage of the prior art technologies of the new proprietary systems providers arises due to the need to discard all prior technologies, and implement an entirely new form of security system to access the new functionalities associated with broadband and wireless data networks. There remains, therefore, a need for systems, devices, and methods that easily interface to and control the existing proprietary security technologies utilizing a variety of wireless technologies.

INCORPORATION BY REFERENCE

Each patent, patent application, and/or publication mentioned in this specification is herein incorporated by reference in its entirety to the same extent as if each individual patent, patent application, and/or publication was specifically and individually indicated to be incorporated by reference.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of the integrated security system, under an embodiment.

FIG. **2** is a block diagram of components of the integrated security system, under an embodiment.

FIG. **3** is a block diagram of the gateway software or applications, under an embodiment.

FIG. **4** is a block diagram of the gateway components, under an embodiment.

FIG. **5** is a block diagram of IP device integration with a premise network, under an embodiment.

FIG. **6** is a block diagram of IP device integration with a premise network, under an alternative embodiment.

FIG. **7** is a block diagram of a touchscreen, under an embodiment.

FIG. **8** is an example screenshot of a networked security touchscreen, under an embodiment.

FIG. **9** is a block diagram of network or premise device integration with a premise network, under an embodiment.

FIG. **10** is a block diagram of network or premise device integration with a premise network, under an alternative embodiment.

FIG. **11** is a flow diagram for installation of an IP device into a private network environment, under an embodiment.

FIG. **12** is a block diagram showing communications among IP devices of the private network environment, under an embodiment.

FIG. **13** is a data flow diagram for a panic alarm, under an embodiment.

FIG. **14** is a data flow diagram for device installation, under an embodiment.

FIG. **15** is a data flow diagram for a camera event, under an embodiment.

FIG. **16** is a flow diagram of a method of integrating an external control and management application system with an existing security system, under an embodiment.

FIG. **17** is a block diagram of an integrated security system wirelessly interfacing to proprietary security systems, under an embodiment.

FIG. **18** is a flow diagram for wirelessly 'learning' the gateway into an existing security system and discovering extant sensors, under an embodiment.

DETAILED DESCRIPTION

An integrated security system is described that integrates broadband and mobile access and control with conventional security systems and premise devices to provide a tri-mode security network (broadband, cellular/GSM, POTS access) that enables users to remotely stay connected to their premises. The integrated security system, while delivering remote premise monitoring and control functionality to conventional monitored premise protection, complements existing premise protection equipment. The integrated security system integrates into the premise network and couples wirelessly with the conventional security panel, enabling broadband access to premise security systems. Automation devices (cameras, lamp modules, thermostats, etc.) can be added, enabling users to remotely see live video and/or pictures and control home devices via their personal web portal or webpage, mobile phone, and/or other remote client device. Users can also receive notifications via email or text message when happenings occur, or do not occur, in their home.

Although the detailed description herein contains many specifics for the purposes of illustration, anyone of ordinary skill in the art will appreciate that many variations and alterations to the following details are within the scope of the embodiments described herein. Thus, the following illustrative embodiments are set forth without any loss of generality to, and without imposing limitations upon, the claimed invention.

In accordance with the embodiments described herein, a wireless system (e.g., radio frequency (RF)) is provided that enables a security provider or consumer to extend the capabilities of an existing RF-capable security system or a non-RF-capable security system that has been upgraded to support RF capabilities. The system includes an RF-capable Gateway device (physically located within RF range of the RF-capable security system) and associated software operating on the Gateway device. The system also includes a web server, application server, and remote database providing a persistent store for information related to the system.

The security systems of an embodiment, referred to herein as the iControl security system or integrated security system, extend the value of traditional home security by adding broadband access and the advantages of remote home monitoring and home control through the formation of a security network including components of the integrated security system integrated with a conventional premise security system and a premise local area network (LAN). With the integrated security system, conventional home security sensors, cameras, touchscreen keypads, lighting controls, and/or Internet Protocol (IP) devices in the home (or business) become connected devices that are accessible anywhere in the world from a web browser, mobile phone or through content-enabled touchscreens. The integrated security system experience allows security operators to both extend the value proposition of their monitored security systems and reach new consumers that include broadband users interested in staying connected to their family, home and property when they are away from home.

The integrated security system of an embodiment includes security servers (also referred to herein as iConnect servers or security network servers) and an iHub gateway (also referred to herein as the gateway, the iHub, or the iHub client) that couples or integrates into a home network (e.g., LAN) and communicates directly with the home security panel, in both wired and wireless installations. The security system of an embodiment automatically discovers the security system components (e.g., sensors, etc.) belonging to the security system and connected to a control panel of the security system and provides consumers with full two-way access via web and mobile portals. The gateway supports various wireless protocols and can interconnect with a wide range of control panels offered by security system providers. Service providers and users can then extend the system's capabilities with the additional IP cameras, lighting modules or security devices such as interactive touchscreen keypads. The integrated security system adds an enhanced value to these security systems by enabling consumers to stay connected through email and SMS alerts, photo push, event-based video capture and rule-based monitoring and notifications. This solution extends the reach of home security to households with broadband access.

The integrated security system builds upon the foundation afforded by traditional security systems by layering broadband and mobile access, IP cameras, interactive touchscreens, and an open approach to home automation on top of traditional security system configurations. The integrated security system is easily installed and managed by the security operator, and simplifies the traditional security installation process, as described below.

The integrated security system provides an open systems solution to the home security market. As such, the foundation of the integrated security system customer premises equipment (CPE) approach has been to abstract devices, and allows applications to manipulate and manage multiple devices from any vendor. The integrated security system DeviceConnect technology that enables this capability supports protocols, devices, and panels from GE Security and Honeywell, as well as consumer devices using Z-Wave, IP cameras (e.g., Ethernet, wifi, and Homeplug), and IP touchscreens. The DeviceConnect is a device abstraction layer that enables any device or protocol layer to interoperate with integrated security system components. This architecture enables the addition of new devices supporting any of these interfaces, as well as add entirely new protocols.

The benefit of DeviceConnect is that it provides supplier flexibility. The same consistent touchscreen, web, and mobile user experience operate unchanged on whatever security equipment selected by a security system provider, with the system provider's choice of IP cameras, backend data center and central station software.

The integrated security system provides a complete system that integrates or layers on top of a conventional host security system available from a security system provider. The security system provider therefore can select different components or configurations to offer (e.g., CDMA, GPRS, no cellular, etc.) as well as have iControl modify the integrated security system configuration for the system provider's specific needs (e.g., change the functionality of the web or mobile portal, add a GE or Honeywell-compatible TouchScreen, etc.).

The integrated security system integrates with the security system provider infrastructure for central station reporting directly via Broadband and GPRS alarm transmissions. Traditional dial-up reporting is supported via the standard panel connectivity. Additionally, the integrated security system provides interfaces for advanced functionality to the CMS, including enhanced alarm events, system installation optimizations, system test verification, video verification, 2-way voice over IP and GSM.

The integrated security system is an IP centric system that includes broadband connectivity so that the gateway augments the existing security system with broadband and GPRS connectivity. If broadband is down or unavailable GPRS may be used, for example. The integrated security system supports GPRS connectivity using an optional wireless package that includes a GPRS modem in the gateway. The integrated security system treats the GPRS connection as a higher cost though flexible option for data transfers. In an embodiment the GPRS connection is only used to route alarm events (e.g., for cost), however the gateway can be configured (e.g., through the iConnect server interface) to act as a primary channel and pass any or all events over GPRS. Consequently, the integrated security system does not interfere with the current plain old telephone service (POTS) security panel interface. Alarm events can still be routed through POTS; however the gateway also allows such events to be routed through a broadband or GPRS connection as well. The integrated security system provides a web application interface to the CSR tool suite as well as XML web services interfaces for programmatic integration between the security system provider's existing call center products. The integrated security system includes, for example, APIs that allow the security system provider to integrate components of the integrated security system into a custom call center interface. The APIs include XML web service APIs for integration of existing security system provider call center applications with the integrated security system service. All functionality available in the CSR Web application is provided with these API sets. The Java and XML-based APIs of the integrated security system support provisioning, billing, system administration, CSR, central station, portal user interfaces, and content management functions, to name a few. The integrated security system can provide a customized interface to the security system provider's billing system, or alternatively can provide security system developers with APIs and support in the integration effort.

The integrated security system provides or includes business component interfaces for provisioning, administration, and customer care to name a few. Standard templates and examples are provided with a defined customer professional services engagement to help integrate OSS/BSS systems of a Service Provider with the integrated security system.

The integrated security system components support and allow for the integration of customer account creation and deletion with a security system. The iConnect APIs provides access to the provisioning and account management system in iConnect and provide full support for account creation, provisioning, and deletion. Depending on the requirements of the security system provider, the iConnect APIs can be used to completely customize any aspect of the integrated security system backend operational system.

The integrated security system includes a gateway that supports the following standards-based interfaces, to name a few: Ethernet IP communications via Ethernet ports on the gateway, and standard XML/TCP/IP protocols and ports are employed over secured SSL sessions; USB 2.0 via ports on the gateway; 802.11b/g/n IP communications; GSM/GPRS RF WAN communications; CDMA 1xRTT RF WAN communications (optional, can also support EVDO and 3G technologies).

The gateway supports the following proprietary interfaces, to name a few: interfaces including Dialog RF network (319.5 MHz) and RS485 Superbus 2000 wired interface; RF mesh network (908 MHz); and interfaces including RF network (345 MHz) and RS485/RS232 bus wired interfaces.

Regarding security for the IP communications (e.g., authentication, authorization, encryption, anti-spoofing, etc), the integrated security system uses SSL to encrypt all IP traffic, using server and client-certificates for authentication, as well as authentication in the data sent over the SSL-encrypted channel. For encryption, integrated security system issues public/private key pairs at the time/place of manufacture, and certificates are not stored in any online storage in an embodiment.

The integrated security system does not need any special rules at the customer premise and/or at the security system provider central station because the integrated security system makes outgoing connections using TCP over the standard HTTP and HTTPS ports. Provided outbound TCP connections are allowed then no special requirements on the firewalls are necessary.

FIG. **1** is a block diagram of the integrated security system **100**, under an embodiment. The integrated security system **100** of an embodiment includes the gateway **102** and the security servers **104** coupled to the conventional home security system **110**. At a customer's home or business, the gateway **102** connects and manages the diverse variety of home security and self-monitoring devices. The gateway **102** communicates with the iConnect Servers **104** located in the service provider's data center **106** (or hosted in integrated security system data center), with the communication taking place via a communication network **108** or other network (e.g., cellular network, internet, etc.). These servers **104** manage the system integrations necessary to deliver the integrated system service described herein. The combination of the gateway **102** and the iConnect servers **104** enable a wide variety of remote client devices **120** (e.g., PCs, mobile phones and PDAs) allowing users to remotely stay in touch with their home, business and family. In addition, the technology allows home security and self-monitoring information, as well as relevant third party content such as traffic and weather, to be presented in intuitive ways within the home, such as on advanced touchscreen keypads.

The integrated security system service (also referred to as iControl service) can be managed by a service provider via browser-based Maintenance and Service Management applications that are provided with the iConnect Servers. Or, if desired, the service can be more tightly integrated with existing OSS/BSS and service delivery systems via the iConnect web services-based XML APIs.

The integrated security system service can also coordinate the sending of alarms to the home security Central Monitoring Station (CMS) **199**. Alarms are passed to the CMS **199** using standard protocols such as Contact ID or SIA and can be generated from the home security panel location as well as by iConnect server **104** conditions (such as lack of communications with the integrated security system). In addition, the link between the security servers **104** and CMS **199** provides tighter integration between home security and self-monitoring devices and the gateway **102**. Such integration enables advanced security capabilities such as the ability for CMS personnel to view photos taken at the time a burglary alarm was triggered. For maximum security, the gateway **102** and iConnect servers **104** support the use of a mobile network (both GPRS and CDMA options are available) as a backup to the primary broadband connection.

The integrated security system service is delivered by hosted servers running software components that communicate with a variety of client types while interacting with other systems. FIG. **2** is a block diagram of components of the integrated security system **100**, under an embodiment. Following is a more detailed description of the components.

The iConnect servers **104** support a diverse collection of clients **120** ranging from mobile devices, to PCs, to in-home security devices, to a service provider's internal systems. Most clients **120** are used by end-users, but there are also a number of clients **120** that are used to operate the service.

Clients **120** used by end-users of the integrated security system **100** include, but are not limited to, the following:

- Clients based on gateway client applications **202** (e.g., a processor-based device running the gateway technology that manages home security and automation devices).
- A web browser **204** accessing a Web Portal application, performing end-user configuration and customization of the integrated security system service as well as monitoring of in-home device status, viewing photos and video, etc. Device and user management can also be performed by this portal application.
- A mobile device **206** (e.g., PDA, mobile phone, etc.) accessing the integrated security system Mobile Portal. This type of client **206** is used by end-users to view system status and perform operations on devices (e.g., turning on a lamp, arming a security panel, etc.) rather than for system configuration tasks such as adding a new device or user.
- PC or browser-based "widget" containers **208** that present integrated security system service content, as well as other third-party content, in simple, targeted ways (e.g. a widget that resides on a PC desktop and shows live video from a single in-home camera). "Widget" as used herein means applications or programs in the system.
- Touchscreen home security keypads **208** and advanced in-home devices that present a variety of content widgets via an intuitive touchscreen user interface.
- Notification recipients **210** (e.g., cell phones that receive SMS-based notifications when certain events occur (or don't occur), email clients that receive an email message with similar information, etc.).
- Custom-built clients (not shown) that access the iConnect web services XML API to interact with users' home security and self-monitoring information in new and unique ways. Such clients could include new types of mobile devices, or complex applications where integrated security system content is integrated into a broader set of application features.

In addition to the end-user clients, the iConnect servers **104** support PC browser-based Service Management clients that manage the ongoing operation of the overall service. These clients run applications that handle tasks such as provisioning, service monitoring, customer support and reporting.

There are numerous types of server components of the iConnect servers **104** of an embodiment including, but not limited to, the following: Business Components which manage information about all of the home security and self-monitoring devices; End-User Application Components which display that information for users and access the Business Components via published XML APIs; and Service Management Application Components which enable operators to administer the service (these components also access the Business Components via the XML APIs, and also via published SNMP MIBs).

The server components provide access to, and management of, the objects associated with an integrated security system installation. The top-level object is the "network." It is a location where a gateway **102** is located, and is also commonly referred to as a site or premises; the premises can include any type of structure (e.g., home, office, warehouse, etc.) at which a gateway **102** is located. Users can only access the networks to which they have been granted permission. Within a network, every object monitored by the gateway **102** is called a device. Devices include the sensors, cameras, home security panels and automation devices, as well as the controller or processor-based device running the gateway applications.

Various types of interactions are possible between the objects in a system. Automations define actions that occur as a result of a change in state of a device. For example, take a picture with the front entry camera when the front door sensor changes to "open". Notifications are messages sent to users to indicate that something has occurred, such as the front door going to "open" state, or has not occurred (referred to as an iWatch notification). Schedules define changes in device states that are to take place at predefined days and times. For example, set the security panel to "Armed" mode every weeknight at 11:00 pm.

The iConnect Business Components are responsible for orchestrating all of the low-level service management activities for the integrated security system service. They define all of the users and devices associated with a network (site), analyze how the devices interact, and trigger associated actions (such as sending notifications to users). All changes in device states are monitored and logged. The Business Components also manage all interactions with external systems as required, including sending alarms and other related self-monitoring data to the home security Central Monitoring System (CMS) **199**. The Business Components are implemented as portable Java J2EE Servlets, but are not so limited.

The following iConnect Business Components manage the main elements of the integrated security system service, but the embodiment is not so limited:

- A Registry Manager **220** defines and manages users and networks. This component is responsible for the creation, modification and termination of users and networks. It is also where a user's access to networks is defined.
- A Network Manager **222** defines and manages security and self-monitoring devices that are deployed on a network (site). This component handles the creation, modification, deletion and configuration of the devices, as well as

the creation of automations, schedules and notification rules associated with those devices.

A Data Manager **224** manages access to current and logged state data for an existing network and its devices. This component specifically does not provide any access to network management capabilities, such as adding new devices to a network, which are handled exclusively by the Network Manager **222**.

To achieve optimal performance for all types of queries, data for current device states is stored separately from historical state data (a.k.a. "logs") in the database. A Log Data Manager **226** performs ongoing transfers of current device state data to the historical data log tables.

Additional iConnect Business Components handle direct communications with certain clients and other systems, for example:

An iHub Manager **228** directly manages all communications with gateway clients, including receiving information about device state changes, changing the configuration of devices, and pushing new versions of the gateway client to the hardware it is running on.

A Notification Manager **230** is responsible for sending all notifications to clients via SMS (mobile phone messages), email (via a relay server like an SMTP email server), etc.

An Alarm and CMS Manager **232** sends critical server-generated alarm events to the home security Central Monitoring Station (CMS) and manages all other communications of integrated security system service data to and from the CMS.

The Element Management System (EMS) **234** is an iControl Business Component that manages all activities associated with service installation, scaling and monitoring, and filters and packages service operations data for use by service management applications. The SNMP MIBs published by the EMS can also be incorporated into any third party monitoring system if desired.

The iConnect Business Components store information about the objects that they manage in the iControl Service Database **240** and in the iControl Content Store **242**. The iControl Content Store is used to store media objects like video, photos and widget content, while the Service Database stores information about users, networks, and devices. Database interaction is performed via a JDBC interface. For security purposes, the Business Components manage all data storage and retrieval.

The iControl Business Components provide web services-based APIs that application components use to access the Business Components' capabilities. Functions of application components include presenting integrated security system service data to end-users, performing administrative duties, and integrating with external systems and back-office applications.

The primary published APIs for the iConnect Business Components include, but are not limited to, the following:

A Registry Manager API **252** provides access to the Registry Manager Business Component's functionality, allowing management of networks and users.

A Network Manager API **254** provides access to the Network Manager Business Component's functionality, allowing management of devices on a network.

A Data Manager API **256** provides access to the Data Manager Business Component's functionality, such as setting and retrieving (current and historical) data about device states.

A Provisioning API **258** provides a simple way to create new networks and configure initial default properties.

Each API of an embodiment includes two modes of access: Java API or XML API. The XML APIs are published as web services so that they can be easily accessed by applications or servers over a network. The Java APIs are a programmer-friendly wrapper for the XML APIs. Application components and integrations written in Java should generally use the Java APIs rather than the XML APIs directly.

The iConnect Business Components also have an XML-based interface **260** for quickly adding support for new devices to the integrated security system. This interface **260**, referred to as DeviceConnect **260**, is a flexible, standards-based mechanism for defining the properties of new devices and how they can be managed. Although the format is flexible enough to allow the addition of any type of future device, pre-defined XML profiles are currently available for adding common types of devices such as sensors (SensorConnect), home security panels (PanelConnect) and IP cameras (CameraConnect).

The iConnect End-User Application Components deliver the user interfaces that run on the different types of clients supported by the integrated security system service. The components are written in portable Java J2EE technology (e.g., as Java Servlets, as JavaServer Pages (JSPs), etc.) and they all interact with the iControl Business Components via the published APIs.

The following End-User Application Components generate CSS-based HTML/JavaScript that is displayed on the target client. These applications can be dynamically branded with partner-specific logos and URL links (such as Customer Support, etc.). The End-User Application Components of an embodiment include, but are not limited to, the following:

An iControl Activation Application **270** that delivers the first application that a user sees when they set up the integrated security system service. This wizard-based web browser application securely associates a new user with a purchased gateway and the other devices included with it as a kit (if any). It primarily uses functionality published by the Provisioning API.

An iControl Web Portal Application **272** runs on PC browsers and delivers the web-based interface to the integrated security system service. This application allows users to manage their networks (e.g. add devices and create automations) as well as to view/change device states, and manage pictures and videos. Because of the wide scope of capabilities of this application, it uses three different Business Component APIs that include the Registry Manager API, Network Manager API, and Data Manager API, but the embodiment is not so limited.

An iControl Mobile Portal **274** is a small-footprint web-based interface that runs on mobile phones and PDAs. This interface is optimized for remote viewing of device states and pictures/videos rather than network management. As such, its interaction with the Business Components is primarily via the Data Manager API.

Custom portals and targeted client applications can be provided that leverage the same Business Component APIs used by the above applications.

A Content Manager Application Component **276** delivers content to a variety of clients. It sends multimedia-rich user interface components to widget container clients (both PC and browser-based), as well as to advanced touchscreen keypad clients. In addition to providing content directly to end-user devices, the Content Manager **276** provides widget-based user interface components to satisfy requests from other Application Components such as the iControl Web **272** and Mobile **274** portals.

A number of Application Components are responsible for overall management of the service. These pre-defined applications, referred to as Service Management Application Components, are configured to offer off-the-shelf solutions for production management of the integrated security system service including provisioning, overall service monitoring, customer support, and reporting, for example. The Service Management Application Components of an embodiment include, but are not limited to, the following:

A Service Management Application **280** allows service administrators to perform activities associated with service installation, scaling and monitoring/alerting. This application interacts heavily with the Element Management System (EMS) Business Component to execute its functionality, and also retrieves its monitoring data from that component via protocols such as SNMP MIBs.

A Kitting Application **282** is used by employees performing service provisioning tasks. This application allows home security and self-monitoring devices to be associated with gateways during the warehouse kitting process.

A CSR Application and Report Generator **284** is used by personnel supporting the integrated security system service, such as CSRs resolving end-user issues and employees enquiring about overall service usage. Pushes of new gateway firmware to deployed gateways is also managed by this application.

The iConnect servers **104** also support custom-built integrations with a service provider's existing OSS/BSS, CSR and service delivery systems **290**. Such systems can access the iConnect web services XML API to transfer data to and from the iConnect servers **104**. These types of integrations can compliment or replace the PC browser-based Service Management applications, depending on service provider needs.

As described above, the integrated security system of an embodiment includes a gateway, or iHub. The gateway of an embodiment includes a device that is deployed in the home or business and couples or connects the various third-party cameras, home security panels, sensors and devices to the iConnect server over a WAN connection as described in detail herein. The gateway couples to the home network and communicates directly with the home security panel in both wired and wireless sensor installations. The gateway is configured to be low-cost, reliable and thin so that it complements the integrated security system network-based architecture.

The gateway supports various wireless protocols and can interconnect with a wide range of home security control panels. Service providers and users can then extend the system's capabilities by adding IP cameras, lighting modules and additional security devices. The gateway is configurable to be integrated into many consumer appliances, including set-top boxes, routers and security panels. The small and efficient footprint of the gateway enables this portability and versatility, thereby simplifying and reducing the overall cost of the deployment.

FIG. **3** is a block diagram of the gateway **102** including gateway software or applications, under an embodiment. The gateway software architecture is relatively thin and efficient, thereby simplifying its integration into other consumer appliances such as set-top boxes, routers, touch screens and security panels. The software architecture also provides a high degree of security against unauthorized access. This section describes the various key components of the gateway software architecture.

The gateway application layer **302** is the main program that orchestrates the operations performed by the gateway. The Security Engine **304** provides robust protection against intentional and unintentional intrusion into the integrated security system network from the outside world (both from inside the premises as well as from the WAN). The Security Engine **304** of an embodiment comprises one or more sub-modules or components that perform functions including, but not limited to, the following:

Encryption including 128-bit SSL encryption for gateway and iConnect server communication to protect user data privacy and provide secure communication.

Bi-directional authentication between the gateway and iConnect server in order to prevent unauthorized spoofing and attacks. Data sent from the iConnect server to the gateway application (or vice versa) is digitally signed as an additional layer of security. Digital signing provides both authentication and validation that the data has not been altered in transit.

Camera SSL encapsulation because picture and video traffic offered by off-the-shelf networked IP cameras is not secure when traveling over the Internet. The gateway provides for 128-bit SSL encapsulation of the user picture and video data sent over the internet for complete user security and privacy.

802.11b/g/n with WPA-2 security to ensure that wireless camera communications always takes place using the strongest available protection.

A gateway-enabled device is assigned a unique activation key for activation with an iConnect server. This ensures that only valid gateway-enabled devices can be activated for use with the specific instance of iConnect server in use. Attempts to activate gateway-enabled devices by brute force are detected by the Security Engine. Partners deploying gateway-enabled devices have the knowledge that only a gateway with the correct serial number and activation key can be activated for use with an iConnect server. Stolen devices, devices attempting to masquerade as gateway-enabled devices, and malicious outsiders (or insiders as knowledgeable but nefarious customers) cannot effect other customers' gateway-enabled devices.

As standards evolve, and new encryption and authentication methods are proven to be useful, and older mechanisms proven to be breakable, the security manager can be upgraded "over the air" to provide new and better security for communications between the iConnect server and the gateway application, and locally at the premises to remove any risk of eavesdropping on camera communications.

A Remote Firmware Download module **306** allows for seamless and secure updates to the gateway firmware through the iControl Maintenance Application on the server **104**, providing a transparent, hassle-free mechanism for the service provider to deploy new features and bug fixes to the installed user base. The firmware download mechanism is tolerant of connection loss, power interruption and user interventions (both intentional and unintentional). Such robustness reduces down time and customer support issues. Gateway firmware can be remotely download either for one gateway at a time, a group of gateways, or in batches.

The Automations engine **308** manages the user-defined rules of interaction between the different devices (e.g. when door opens turn on the light). Though the automation rules are programmed and reside at the portal/server level, they are cached at the gateway level in order to provide short latency between device triggers and actions.

DeviceConnect **310** includes definitions of all supported devices (e.g., cameras, security panels, sensors, etc.) using a standardized plug-in architecture. The DeviceConnect module **310** offers an interface that can be used to quickly add support for any new device as well as enabling interoperability between devices that use different technologies/protocols. For common device types, pre-defined sub-modules have been defined, making supporting new devices of these types even easier. SensorConnect **312** is provided for adding new sensors, CameraConnect **316** for adding IP cameras, and PanelConnect **314** for adding home security panels.

The Schedules engine **318** is responsible for executing the user defined schedules (e.g., take a picture every five minutes; every day at 8 am set temperature to 65 degrees Fahrenheit, etc.). Though the schedules are programmed and reside at the iConnect server level they are sent to the scheduler within the gateway application. The Schedules Engine **318** then interfaces with SensorConnect **312** to ensure that scheduled events occur at precisely the desired time.

The Device Management module **320** is in charge of all discovery, installation and configuration of both wired and wireless IP devices (e.g., cameras, etc.) coupled or connected to the system. Networked IP devices, such as those used in the integrated security system, require user configuration of many IP and security parameters—to simplify the user experience and reduce the customer support burden, the device management module of an embodiment handles the details of this configuration. The device management module also manages the video routing module described below.

The video routing engine **322** is responsible for delivering seamless video streams to the user with zero-configuration. Through a multi-step, staged approach the video routing engine uses a combination of UPnP port-forwarding, relay server routing and STUN/TURN peer-to-peer routing.

FIG. **4** is a block diagram of components of the gateway **102**, under an embodiment. Depending on the specific set of functionality desired by the service provider deploying the integrated security system service, the gateway **102** can use any of a number of processors **402**, due to the small footprint of the gateway application firmware. In an embodiment, the gateway could include the Broadcom BCM5354 as the processor for example. In addition, the gateway **102** includes memory (e.g., FLASH **404**, RAM **406**, etc.) and any number of input/output (I/O) ports **408**.

Referring to the WAN portion **410** of the gateway **102**, the gateway **102** of an embodiment can communicate with the iConnect server using a number of communication types and/or protocols, for example Broadband **412**, GPRS **414** and/or Public Switched Telephone Network (PTSN) **416** to name a few. In general, broadband communication **412** is the primary means of connection between the gateway **102** and the iConnect server **104** and the GPRS/CDMA **414** and/or PSTN **416** interfaces acts as back-up for fault tolerance in case the user's broadband connection fails for whatever reason, but the embodiment is not so limited.

Referring to the LAN portion **420** of the gateway **102**, various protocols and physical transceivers can be used to communicate to off-the-shelf sensors and cameras. The gateway **102** is protocol-agnostic and technology-agnostic and as such can easily support almost any device networking protocol. The gateway **102** can, for example, support GE and Honeywell security RF protocols **422**, Z-Wave **424**, serial (RS232 and RS485) 426 for direct connection to security panels as well as WiFi 428 (802.11b/g) for communication to WiFi cameras.

The integrated security system includes couplings or connections among a variety of IP devices or components, and the device management module is in charge of the discovery, installation and configuration of the IP devices coupled or connected to the system, as described above. The integrated security system of an embodiment uses a "sandbox" network to discover and manage all IP devices coupled or connected as components of the system. The IP devices of an embodiment include wired devices, wireless devices, cameras, interactive touchscreens, and security panels to name a few. These devices can be wired via ethernet cable or Wifi devices, all of which are secured within the sandbox network, as described below. The "sandbox" network is described in detail below.

FIG. **5** is a block diagram **500** of network or premise device integration with a premise network **250**, under an embodiment. In an embodiment, network devices **255-257** are coupled to the gateway **102** using a secure network coupling or connection such as SSL over an encrypted 802.11 link (utilizing for example WPA-2 security for the wireless encryption). The network coupling or connection between the gateway **102** and the network devices **255-257** is a private coupling or connection in that it is segregated from any other network couplings or connections. The gateway **102** is coupled to the premise router/firewall **252** via a coupling with a premise LAN **250**. The premise router/firewall **252** is coupled to a broadband modem **251**, and the broadband modem **251** is coupled to a WAN **200** or other network outside the premise. The gateway **102** thus enables or forms a separate wireless network, or sub-network, that includes some number of devices and is coupled or connected to the LAN **250** of the host premises. The gateway sub-network can include, but is not limited to, any number of other devices like WiFi IP cameras, security panels (e.g., IP-enabled), and security touchscreens, to name a few. The gateway **102** manages or controls the sub-network separately from the LAN **250** and transfers data and information between components of the sub-network and the LAN **250**/WAN **200**, but is not so limited. Additionally, other network devices **254** can be coupled to the LAN **250** without being coupled to the gateway **102**.

FIG. **6** is a block diagram **600** of network or premise device integration with a premise network **250**, under an alternative embodiment. The network or premise devices **255-257** are coupled to the gateway **102**. The network coupling or connection between the gateway **102** and the network devices **255-257** is a private coupling or connection in that it is segregated from any other network couplings or connections. The gateway **102** is coupled or connected between the premise router/firewall **252** and the broadband modem **251**. The broadband modem **251** is coupled to a WAN **200** or other network outside the premise, while the premise router/firewall **252** is coupled to a premise LAN **250**. As a result of its location between the broadband modem **251** and the premise router/firewall **252**, the gateway **102** can be configured or function as the premise router routing specified data between the outside network (e.g., WAN **200**) and the premise router/firewall **252** of the LAN **250**. As described above, the gateway **102** in this configuration enables or forms a separate wireless network, or sub-network, that includes the network or premise devices **255-257** and is coupled or connected between the LAN **250** of the host premises and the WAN **200**. The gateway sub-network can include, but is not limited to, any number of network or premise devices **255-257** like WiFi IP cameras, security panels (e.g., IP-enabled), and security touchscreens, to name a few. The gateway **102** manages or controls the sub-network separately from the LAN **250** and transfers data and information between components of the sub-network and the LAN **250**/WAN **200**, but is not so limited. Additionally, other network devices **254** can be coupled to the LAN **250** without being coupled to the gateway **102**.

The examples described above with reference to FIGS. **5** and **6** are presented only as examples of IP device integration. The integrated security system is not limited to the type, number and/or combination of IP devices shown and described in these examples, and any type, number and/or combination of IP devices is contemplated within the scope of this disclosure as capable of being integrated with the premise network.

The integrated security system of an embodiment includes a touchscreen (also referred to as the iControl touchscreen or integrated security system touchscreen), as described above, which provides core security keypad functionality, content management and presentation, and embedded systems design. The networked security touchscreen system of an embodiment enables a consumer or security provider to easily and automatically install, configure and manage the security system and touchscreen located at a customer premise. Using this system the customer may access and control the local security system, local IP devices such as cameras, local sensors and control devices (such as lighting controls or pipe freeze sensors), as well as the local security system panel and associated security sensors (such as door/window, motion, and smoke detectors). The customer premise may be a home, business, and/or other location equipped with a wired or wireless broadband IP connection.

The system of an embodiment includes a touchscreen with a configurable software user interface and/or a gateway device (e.g., iHub) that couples or connects to a premise security panel through a wired or wireless connection, and a remote server that provides access to content and information from the premises devices to a user when they are remote from the home. The touchscreen supports broadband and/or WAN wireless connectivity. In this embodiment, the touchscreen incorporates an IP broadband connection (e.g., Wifi radio, Ethernet port, etc.), and/or a cellular radio (e.g., GPRS/GSM, CDMA, WiMax, etc.). The touchscreen described herein can be used as one or more of a security system interface panel and a network user interface (UI) that provides an interface to interact with a network (e.g., LAN, WAN, internet, etc.).

The touchscreen of an embodiment provides an integrated touchscreen and security panel as an all-in-one device. Once integrated using the touchscreen, the touchscreen and a security panel of a premise security system become physically co-located in one device, and the functionality of both may even be co-resident on the same CPU and memory (though this is not required).

The touchscreen of an embodiment also provides an integrated IP video and touchscreen UI. As such, the touchscreen supports one or more standard video CODECs/players (e.g., H.264, Flash Video, MOV, MPEG4, M-JPEG, etc.). The touchscreen UI then provides a mechanism (such as a camera or video widget) to play video. In an embodiment the video is streamed live from an IP video camera. In other embodiments the video comprises video clips or photos sent from an IP camera or from a remote location.

The touchscreen of an embodiment provides a configurable user interface system that includes a configuration supporting use as a security touchscreen. In this embodiment, the touchscreen utilizes a modular user interface that allows components to be modified easily by a service provider, an installer, or even the end user. Examples of such a modular approach include using Flash widgets, HTML-based widgets, or other downloadable code modules such that the user interface of the touchscreen can be updated and modified while the application is running. In an embodiment the touchscreen user interface modules can be downloaded over the internet. For example, a new security configuration widget can be downloaded from a standard web server, and the touchscreen then loads such configuration app into memory, and inserts it in place of the old security configuration widget. The touchscreen of an embodiment is configured to provide a self-install user interface.

Embodiments of the networked security touchscreen system described herein include a touchscreen device with a user interface that includes a security toolbar providing one or more functions including arm, disarm, panic, medic, and alert. The touchscreen therefore includes at least one screen having a separate region of the screen dedicated to a security toolbar. The security toolbar of an embodiment is present in the dedicated region at all times that the screen is active.

The touchscreen of an embodiment includes a home screen having a separate region of the screen allocated to managing home-based functions. The home-based functions of an embodiment include managing, viewing, and/or controlling IP video cameras. In this embodiment, regions of the home screen are allocated in the form of widget icons; these widget icons (e.g. for cameras, thermostats, lighting, etc) provide functionality for managing home systems. So, for example, a displayed camera icon, when selected, launches a Camera Widget, and the Camera widget in turn provides access to video from one or more cameras, as well as providing the user with relevant camera controls (take a picture, focus the camera, etc.)

The touchscreen of an embodiment includes a home screen having a separate region of the screen allocated to managing, viewing, and/or controlling internet-based content or applications. For example, the Widget Manager UI presents a region of the home screen (up to and including the entire home screen) where internet widgets icons such as weather, sports, etc. may be accessed). Each of these icons may be selected to launch their respective content services.

The touchscreen of an embodiment is integrated into a premise network using the gateway, as described above. The gateway as described herein functions to enable a separate wireless network, or sub-network, that is coupled, connected, or integrated with another network (e.g., WAN, LAN of the host premises, etc.). The sub-network enabled by the gateway optimizes the installation process for IP devices, like the touchscreen, that couple or connect to the sub-network by segregating these IP devices from other such devices on the network. This segregation of the IP devices of the sub-network further enables separate security and privacy policies to be implemented for these IP devices so that, where the IP devices are dedicated to specific functions (e.g., security), the security and privacy policies can be tailored specifically for the specific functions. Furthermore, the gateway and the sub-network it forms enables the segregation of data traffic, resulting in faster and more efficient data flow between components of the host network, components of the sub-network, and between components of the sub-network and components of the network.

The touchscreen of an embodiment includes a core functional embedded system that includes an embedded operating system, required hardware drivers, and an open system interface to name a few. The core functional embedded system can be provided by or as a component of a conventional security system (e.g., security system available from GE Security). These core functional units are used with components of the integrated security system as described herein. Note that portions of the touchscreen description below may include reference to a host premise security system (e.g., GE security system), but these references are included only as an example and do not limit the touchscreen to integration with any particular security system.

As an example, regarding the core functional embedded system, a reduced memory footprint version of embedded

Linux forms the core operating system in an embodiment, and provides basic TCP/IP stack and memory management functions, along with a basic set of low-level graphics primitives. A set of device drivers is also provided or included that offer low-level hardware and network interfaces. In addition to the tandard drivers, an interface to the RS 485 bus is included that couples or connects to the security system panel (e.g., GE Concord panel). The interface may, for example, implement the Superbus 2000 protocol, which can then be utilized by the more comprehensive transaction-level security functions implemented in PanelConnect technology (e.g SetAlarmLevel (int level, int partition, char *accessCode)). Power control drivers are also provided.

FIG. **7** is a block diagram of a touchscreen **700** of the integrated security system, under an embodiment. The touchscreen **700** generally includes an application/presentation layer **702** with a resident application **704**, and a core engine **706**. The touchscreen **700** also includes one or more of the following, but is not so limited: applications of premium services **710**, widgets **712**, a caching proxy **714**, network security **716**, network interface **718**, security object **720**, applications supporting devices **722**, PanelConnect API **724**, a gateway interface **726**, and one or more ports **728**.

More specifically, the touchscreen, when configured as a home security device, includes but is not limited to the following application or software modules: RS 485 and/or RS-232 bus security protocols to conventional home security system panel (e.g., GE Concord panel); functional home security classes and interfaces (e.g. Panel ARM state, Sensor status, etc.); Application/Presentation layer or engine; Resident Application; Consumer Home Security Application; installer home security application; core engine; and System bootloader/Software Updater. The core Application engine and system bootloader can also be used to support other advanced content and applications. This provides a seamless interaction between the premise security application and other optional services such as weather widgets or IP cameras.

An alternative configuration of the touchscreen includes a first Application engine for premise security and a second Application engine for all other applications. The integrated security system application engine supports content standards such as HTML, XML, Flash, etc. and enables a rich consumer experience for all 'widgets', whether security-based or not. The touchscreen thus provides service providers the ability to use web content creation and management tools to build and download any 'widgets' regardless of their functionality.

As discussed above, although the Security Applications have specific low-level functional requirements in order to interface with the premise security system, these applications make use of the same fundamental application facilities as any other 'widget', application facilities that include graphical layout, interactivity, application handoff, screen management, and network interfaces, to name a few.

Content management in the touchscreen provides the ability to leverage conventional web development tools, performance optimized for an embedded system, service provider control of accessible content, content reliability in a consumer device, and consistency between 'widgets' and seamless widget operational environment. In an embodiment of the integrated security system, widgets are created by web developers and hosted on the integrated security system Content Manager (and stored in the Content Store database). In this embodiment the server component caches the widgets and offers them to consumers through the web-based integrated security system provisioning system. The servers interact with the advanced touchscreen using HTTPS interfaces controlled by the core engine and dynamically download widgets and updates as needed to be cached on the touchscreen. In other embodiments widgets can be accessed directly over a network such as the Internet without needing to go through the iControl Content Manager

Referring to FIG. **7**, the touchscreen system is built on a tiered architecture, with defined interfaces between the Application/Presentation Layer (the Application Engine) on the top, the Core Engine in the middle, and the security panel and gateway APIs at the lower level. The architecture is configured to provide maximum flexibility and ease of maintenance.

The application engine of the touchscreen provides the presentation and interactivity capabilities for all applications (widgets) that run on the touchscreen, including both core security function widgets and third party content widgets. FIG. **8** is an example screenshot **800** of a networked security touchscreen, under an embodiment. This example screenshot **800** includes three interfaces or user interface (UI) components **802-806**, but is not so limited. A first UI **802** of the touchscreen includes icons by which a user controls or accesses functions and/or components of the security system (e.g., "Main", "Panic", "Medic", "Fire", state of the premise alarm system (e.g., disarmed, armed, etc.), etc.); the first UI **802**, which is also referred to herein as a security interface, is always presented on the touchscreen. A second UI **804** of the touchscreen includes icons by which a user selects or interacts with services and other network content (e.g., clock, calendar, weather, stocks, news, sports, photos, maps, music, etc.) that is accessible via the touchscreen. The second UI **804** is also referred to herein as a network interface or content interface. A third UI **806** of the touchscreen includes icons by which a user selects or interacts with additional services or components (e.g., intercom control, security, cameras coupled to the system in particular regions (e.g., front door, baby, etc.) available via the touchscreen.

A component of the application engine is the Presentation Engine, which includes a set of libraries that implement the standards-based widget content (e.g., XML, HTML, JavaScript, Flash) layout and interactivity. This engine provides the widget with interfaces to dynamically load both graphics and application logic from third parties, support high level data description language as well as standard graphic formats. The set of web content-based functionality available to a widget developer is extended by specific touchscreen functions implemented as local web services by the Core Engine.

The resident application of the touchscreen is the master service that controls the interaction of all widgets in the system, and enforces the business and security rules required by the service provider. For example, the resident application determines the priority of widgets, thereby enabling a home security widget to override resource requests from a less critical widget (e.g. a weather widget). The resident application also monitors widget behavior, and responds to client or server requests for cache updates.

The core engine of the touchscreen manages interaction with other components of the integrated security system, and provides an interface through which the resident application and authorized widgets can get information about the home security system, set alarms, install sensors, etc. At the lower level, the Core Engine's main interactions are through the PanelConnect API, which handles all communication with the security panel, and the gateway Interface, which handles communication with the gateway. In an embodiment, both the iHub Interface and PanelConnect API are resident and operating on the touchscreen. In another embodiment, the Panel-

Connect API runs on the gateway or other device that provides security system interaction and is accessed by the touchscreen through a web services interface.

The Core Engine also handles application and service level persistent and cached memory functions, as well as the dynamic provisioning of content and widgets, including but not limited to: flash memory management, local widget and content caching, widget version management (download, cache flush new/old content versions), as well as the caching and synchronization of user preferences. As a portion of these services the Core engine incorporates the bootloader functionality that is responsible for maintaining a consistent software image on the touchscreen, and acts as the client agent for all software updates. The bootloader is configured to ensure full update redundancy so that unsuccessful downloads cannot corrupt the integrated security system.

Video management is provided as a set of web services by the Core Engine. Video management includes the retrieval and playback of local video feeds as well as remote control and management of cameras (all through iControl CameraConnect technology).

Both the high level application layer and the mid-level core engine of the touchscreen can make calls to the network. Any call to the network made by the application layer is automatically handed off to a local caching proxy, which determines whether the request should be handled locally. Many of the requests from the application layer are web services API requests; although such requests could be satisfied by the iControl servers, they are handled directly by the touchscreen and the gateway. Requests that get through the caching proxy are checked against a white list of acceptable sites, and, if they match, are sent off through the network interface to the gateway. Included in the Network Subsystem is a set of network services including HTTP, HTTPS, and server-level authentication functions to manage the secure client-server interface. Storage and management of certificates is incorporated as a part of the network services layer.

Server components of the integrated security system servers support interactive content services on the touchscreen. These server components include, but are not limited to the content manager, registry manager, network manager, and global registry, each of which is described herein.

The Content Manager oversees aspects of handling widget data and raw content on the touchscreen. Once created and validated by the service provider, widgets are 'ingested' to the Content Manager, and then become available as downloadable services through the integrated security system Content Management APIs. The Content manager maintains versions and timestamp information, and connects to the raw data contained in the backend Content Store database. When a widget is updated (or new content becomes available) all clients registering interest in a widget are systematically updated as needed (a process that can be configured at an account, locale, or system-wide level).

The Registry Manager handles user data, and provisioning accounts, including information about widgets the user has decided to install, and the user preferences for these widgets.

The Network Manager handles getting and setting state for all devices on the integrated security system network (e.g., sensors, panels, cameras, etc.). The Network manager synchronizes with the gateway, the advanced touchscreen, and the subscriber database.

The Global Registry is a primary starting point server for all client services, and is a logical referral service that abstracts specific server locations/addresses from clients (touchscreen, gateway **102**, desktop widgets, etc.). This approach enables easy scaling/migration of server farms.

The touchscreen of an embodiment operates wirelessly with a premise security system. The touchscreen of an embodiment incorporates an RF transceiver component that either communicates directly with the sensors and/or security panel over the panel's proprietary RF frequency, or the touchscreen communicates wirelessly to the gateway over 802.11, Ethernet, or other IP-based communications channel, as described in detail herein. In the latter case the gateway implements the PanelConnect interface and communicates directly to the security panel and/or sensors over wireless or wired networks as described in detail above.

The touchscreen of an embodiment is configured to operate with multiple security systems through the use of an abstracted security system interface. In this embodiment, the PanelConnect API can be configured to support a plurality of proprietary security system interfaces, either simultaneously or individually as described herein. In one embodiment of this approach, the touchscreen incorporates multiple physical interfaces to security panels (e.g. GE Security RS-485, Honeywell RF, etc.) in addition to the PanelConnect API implemented to support multiple security interfaces. The change needed to support this in PanelConnect is a configuration parameter specifying the panel type connection that is being utilized.

So for example, the setARMState( ) function is called with an additional parameter (e.g., Armstate=setARMState (type="ARM STAY|ARM AWAY|DISARM", Parameters="ExitDelay=30|Lights=OFF", panelType="GE Concord4 RS485")). The 'panelType' parameter is used by the setARMState function (and in practice by all of the PanelConnect functions) to select an algorithm appropriate to the specific panel out of a plurality of alogorithms.

The touchscreen of an embodiment is self-installable. Consequently, the touchscreen provides a 'wizard' approach similar to that used in traditional computer installations (e.g. InstallShield). The wizard can be resident on the touchscreen, accessible through a web interface, or both. In one embodiment of a touchscreen self-installation process, the service provider can associate devices (sensors, touchscreens, security panels, lighting controls, etc.) remotely using a web-based administrator interface.

The touchscreen of an embodiment includes a battery backup system for a security touchscreen. The touchscreen incorporates a standard Li-ion or other battery and charging circuitry to allow continued operation in the event of a power outage. In an embodiment the battery is physically located and connected within the touchscreen enclosure. In another embodiment the battery is located as a part of the power transformer, or in between the power transformer and the touchscreen.

The example configurations of the integrated security system described above with reference to FIGS. **5** and **6** include a gateway that is a separate device, and the touchscreen couples to the gateway. However, in an alternative embodiment, the gateway device and its functionality can be incorporated into the touchscreen so that the device management module, which is now a component of or included in the touchscreen, is in charge of the discovery, installation and configuration of the IP devices coupled or connected to the system, as described above. The integrated security system with the integrated touchscreen/gateway uses the same "sandbox" network to discover and manage all IP devices coupled or connected as components of the system.

The touchscreen of this alternative embodiment integrates the components of the gateway with the components of the touchscreen as described herein. More specifically, the touchscreen of this alternative embodiment includes software or applications described above with reference to FIG. **3**. In this alternative embodiment, the touchscreen includes the gateway application layer **302** as the main program that orchestrates the operations performed by the gateway. A Security Engine **304** of the touchscreen provides robust protection against intentional and unintentional intrusion into the integrated security system network from the outside world (both from inside the premises as well as from the WAN). The Security Engine **304** of an embodiment comprises one or more sub-modules or components that perform functions including, but not limited to, the following:

- Encryption including 128-bit SSL encryption for gateway and iConnect server communication to protect user data privacy and provide secure communication.
- Bi-directional authentication between the touchscreen and iConnect server in order to prevent unauthorized spoofing and attacks. Data sent from the iConnect server to the gateway application (or vice versa) is digitally signed as an additional layer of security. Digital signing provides both authentication and validation that the data has not been altered in transit.
- Camera SSL encapsulation because picture and video traffic offered by off-the-shelf networked IP cameras is not secure when traveling over the Internet. The touchscreen provides for 128-bit SSL encapsulation of the user picture and video data sent over the internet for complete user security and privacy.
- 802.11b/g/n with WPA-2 security to ensure that wireless camera communications always takes place using the strongest available protection.
- A touchscreen-enabled device is assigned a unique activation key for activation with an iConnect server. This ensures that only valid gateway-enabled devices can be activated for use with the specific instance of iConnect server in use. Attempts to activate gateway-enabled devices by brute force are detected by the Security Engine. Partners deploying touchscreen-enabled devices have the knowledge that only a gateway with the correct serial number and activation key can be activated for use with an iConnect server. Stolen devices, devices attempting to masquerade as gateway-enabled devices, and malicious outsiders (or insiders as knowledgeable but nefarious customers) cannot effect other customers' gateway-enabled devices.

As standards evolve, and new encryption and authentication methods are proven to be useful, and older mechanisms proven to be breakable, the security manager can be upgraded "over the air" to provide new and better security for communications between the iConnect server and the gateway application, and locally at the premises to remove any risk of eavesdropping on camera communications.

A Remote Firmware Download module **306** of the touchscreen allows for seamless and secure updates to the gateway firmware through the iControl Maintenance Application on the server **104**, providing a transparent, hassle-free mechanism for the service provider to deploy new features and bug fixes to the installed user base. The firmware download mechanism is tolerant of connection loss, power interruption and user interventions (both intentional and unintentional). Such robustness reduces down time and customer support issues. Touchscreen firmware can be remotely download either for one touchscreen at a time, a group of touchscreen, or in batches.

The Automations engine **308** of the touchscreen manages the user-defined rules of interaction between the different devices (e.g. when door opens turn on the light). Though the automation rules are programmed and reside at the portal/server level, they are cached at the gateway level in order to provide short latency between device triggers and actions.

DeviceConnect **310** of the touchscreen touchscreen includes definitions of all supported devices (e.g., cameras, security panels, sensors, etc.) using a standardized plug-in architecture. The DeviceConnect module **310** offers an interface that can be used to quickly add support for any new device as well as enabling interoperability between devices that use different technologies/protocols. For common device types, pre-defined sub-modules have been defined, making supporting new devices of these types even easier. SensorConnect **312** is provided for adding new sensors, CameraConnect **316** for adding IP cameras, and PanelConnect **314** for adding home security panels.

The Schedules engine **318** of the touchscreen is responsible for executing the user defined schedules (e.g., take a picture every five minutes; every day at 8 am set temperature to 65 degrees Fahrenheit, etc.). Though the schedules are programmed and reside at the iConnect server level they are sent to the scheduler within the gateway application of the touchscreen. The Schedules Engine **318** then interfaces with SensorConnect **312** to ensure that scheduled events occur at precisely the desired time.

The Device Management module **320** of the touchscreen is in charge of all discovery, installation and configuration of both wired and wireless IP devices (e.g., cameras, etc.) coupled or connected to the system. Networked IP devices, such as those used in the integrated security system, require user configuration of many IP and security parameters, and the device management module of an embodiment handles the details of this configuration. The device management module also manages the video routing module described below.

The video routing engine **322** of the touchscreen is responsible for delivering seamless video streams to the user with zero-configuration. Through a multi-step, staged approach the video routing engine uses a combination of UPnP port-forwarding, relay server routing and STUN/TURN peer-to-peer routing.

FIG. **9** is a block diagram **900** of network or premise device integration with a premise network **250**, under an embodiment. In an embodiment, network devices **255**, **256**, **957** are coupled to the touchscreen **902** using a secure network connection such as SSL over an encrypted 802.11 link (utilizing for example WPA-2 security for the wireless encryption), and the touchscreen **902** coupled to the premise router/firewall **252** via a coupling with a premise LAN **250**. The premise router/firewall **252** is coupled to a broadband modem **251**, and the broadband modem **251** is coupled to a WAN **200** or other network outside the premise. The touchscreen **902** thus enables or forms a separate wireless network, or sub-network, that includes some number of devices and is coupled or connected to the LAN **250** of the host premises. The touchscreen sub-network can include, but is not limited to, any number of other devices like WiFi IP cameras, security panels (e.g., IP-enabled), and IP devices, to name a few. The touchscreen **902** manages or controls the sub-network separately from the LAN **250** and transfers data and information between components of the sub-network and the LAN **250**/WAN **200**, but is not so limited. Additionally, other network devices **254** can be coupled to the LAN **250** without being coupled to the touchscreen **902**.

FIG. **10** is a block diagram **1000** of network or premise device integration with a premise network **250**, under an alternative embodiment. The network or premise devices **255**, **256**, **1057** are coupled to the touchscreen **1002**, and the touchscreen **1002** is coupled or connected between the premise router/firewall **252** and the broadband modem **251**. The broadband modem **251** is coupled to a WAN **200** or other network outside the premise, while the premise router/firewall **252** is coupled to a premise LAN **250**. As a result of its location between the broadband modem **251** and the premise router/firewall **252**, the touchscreen **1002** can be configured or function as the premise router routing specified data between the outside network (e.g., WAN **200**) and the premise router/firewall **252** of the LAN **250**. As described above, the touchscreen **1002** in this configuration enables or forms a separate wireless network, or sub-network, that includes the network or premise devices **255**, **156**, **1057** and is coupled or connected between the LAN **250** of the host premises and the WAN **200**. The touchscreen sub-network can include, but is not limited to, any number of network or premise devices **255**, **256**, **1057** like WiFi IP cameras, security panels (e.g., IP-enabled), and security touchscreens, to name a few. The touchscreen **1002** manages or controls the sub-network separately from the LAN **250** and transfers data and information between components of the sub-network and the LAN **250**/WAN **200**, but is not so limited. Additionally, other network devices **254** can be coupled to the LAN **250** without being coupled to the touchscreen **1002**.

The gateway of an embodiment, whether a stand-along component or integrated with a touchscreen, enables couplings or connections and thus the flow or integration of information between various components of the host premises and various types and/or combinations of IP devices, where the components of the host premises include a network (e.g., LAN) and/or a security system or subsystem to name a few. Consequently, the gateway controls the association between and the flow of information or data between the components of the host premises. For example, the gateway of an embodiment forms a sub-network coupled to another network (e.g., WAN, LAN, etc.), with the sub-network including IP devices. The gateway further enables the association of the IP devices of the sub-network with appropriate systems on the premises (e.g., security system, etc.). Therefore, for example, the gateway can form a sub-network of IP devices configured for security functions, and associate the sub-network only with the premises security system, thereby segregating the IP devices dedicated to security from other IP devices that may be coupled to another network on the premises.

In an example embodiment, FIG. **11** is a flow diagram **1100** for integration or installation of an IP device into a private network environment, under an embodiment. The IP device includes any IP-capable device which, for example, includes the touchscreen of an embodiment. The variables of an embodiment set at time of installation include, but are not limited to, one or more of a private SSID/Password, a gateway identifier, a security panel identifier, a user account TS, and a Central Monitoring Station account identification.

An embodiment of the IP device discovery and management begins with a user or installer activating **1102** the gateway and initiating **1104** the install mode of the system. This places the gateway in an install mode. Once in install mode, the gateway shifts to a default (Install) Wifi configuration. This setting will match the default setting for other integrated security system-enabled devices that have been pre-configured to work with the integrated security system. The gateway will then begin to provide **1106** DHCP addresses for these IP devices. Once the devices have acquired a new DHCP address from the gateway, those devices are available for configuration into a new secured Wifi network setting.

The user or installer of the system selects **1108** all devices that have been identified as available for inclusion into the integrated security system. The user may select these devices by their unique IDs via a web page, Touchscreen, or other client interface. The gateway provides **1110** data as appropriate to the devices. Once selected, the devices are configured **1112** with appropriate secured Wifi settings, including SSID and WPA/WPA-2 keys that are used once the gateway switches back to the secured sandbox configuration from the "Install" settings. Other settings are also configured as appropriate for that type of device. Once all devices have been configured, the user is notified and the user can exit install mode. At this point all devices will have been registered **1114** with the integrated security system servers.

The installer switches **1116** the gateway to an operational mode, and the gateway instructs or directs **1118** all newly configured devices to switch to the "secured" Wifi sandbox settings. The gateway then switches **1120** to the "secured" Wifi settings. Once the devices identify that the gateway is active on the "secured" network, they request new DHCP addresses from the gateway which, in response, provides **1122** the new addresses. The devices with the new addresses are then operational **1124** on the secured network.

In order to ensure the highest level of security on the secured network, the gateway can create or generate a dynamic network security configuration based on the unique ID and private key in the gateway, coupled with a randomizing factor that can be based on online time or other inputs. This guarantees the uniqueness of the gateway secured network configuration.

To enable the highest level of performance, the gateway analyzes the RF spectrum of the 802.11x network and determines which frequency band/channel it should select to run.

An alternative embodiment of the camera/IP device management process leverages the local ethernet connection of the sandbox network on the gateway. This alternative process is similar to the Wifi discovery embodiment described above, except the user connects the targeted device to the ethernet port of the sandbox network to begin the process. This alternative embodiment accommodates devices that have not been pre-configured with the default "Install" configuration for the integrated security system.

This alternative embodiment of the IP device discovery and management begins with the user/installer placing the system into install mode. The user is instructed to attach an IP device to be installed to the sandbox Ethernet port of the gateway. The IP device requests a DHCP address from the gateway which, in response to the request, provides the address. The user is presented the device and is asked if he/she wants to install the device. If yes, the system configures the device with the secured Wifi settings and other device-specific settings (e.g., camera settings for video length, image quality etc.). The user is next instructed to disconnect the device from the ethernet port. The device is now available for use on the secured sandbox network.

FIG. **12** is a block diagram showing communications among integrated IP devices of the private network environment, under an embodiment. The IP devices of this example include a security touchscreen **1203**, gateway **1202** (e.g., "iHub"), and security panel (e.g., "Security Panel **1**", "Security Panel **2**", "Security Panel n"), but the embodiment is not so limited. In alternative embodiments any number and/or combination of these three primary component types may be combined with other components including IP devices and/or security system components. For example, a single device which comprises an integrated gateway, touchscreen, and security panel is merely another embodiment of the integrated security system described herein. The description that follows includes an example configuration that includes a touchscreen hosting particular applications. However, the embodiment is not limited to the touchscreen hosting these applications, and the touchscreen should be thought of as representing any IP device.

Referring to FIG. **12**, the touchscreen **1203** incorporates an application **1210** that is implemented as computer code resident on the touchscreen operating system, or as a web-based application running in a browser, or as another type of scripted application (e.g., Flash, Java, Visual Basic, etc.). The touchscreen core application **1210** represents this application, providing user interface and logic for the end user to manage their security system or to gain access to networked information or content (Widgets). The touchscreen core application **1210** in turn accesses a library or libraries of functions to control the local hardware (e.g. screen display, sound, LEDs, memory, etc.) as well as specialized librarie(s) to couple or connect to the security system.

In an embodiment of this security system connection, the touchscreen **1203** communicates to the gateway **1202**, and has no direct communication with the security panel. In this embodiment, the touchscreen core application **1210** accesses the remote service APIs **1212** which provide security system functionality (e.g. ARM/DISARM panel, sensor state, get/set panel configuration parameters, initiate or get alarm events, etc.). In an embodiment, the remote service APIs **1212** implement one or more of the following functions, but the embodiment is not so limited: Armstate=setARMState(type="ARM STAYS ARM AWAY DISARM", Parameters="ExitDelay=30|(Lights=OFF"); sensorState=getSensors (type="ALL|SensorName|SensorNameList"); result=setSensorState(SensorName, parameters="Option**1**, Options**2**, . . . Option n"); interruptHandler=SensorEvent( ) and, interruptHandler=alarmEvent( )

Functions of the remote service APIs **1212** of an embodiment use a remote PanelConnect API **1224** which which resides in memory on the gateway **1202**. The touchscreen **1203** communicates with the gateway **1202** through a suitable network interface such as an Ethernet or 802.11 RF connection, for example. The remote PanelConnect API **1224** provides the underlying Security System Interfaces **1226** used to communicate with and control one or more types of security panel via wired link **1230** and/or RF link **3**. The PanelConnect API **1224** provides responses and input to the remote services APIs **1226**, and in turn translates function calls and data to and from the specific protocols and functions supported by a specific implementation of a Security Panel (e.g. a GE Security Simon XT or Honeywell Vista 20P). In an embodiment, the PanelConnect API **1224** uses a 345 MHz RF transceiver or receiver hardware/firmware module to communicate wirelessly to the security panel and directly to a set of 345 MHz RF-enabled sensors and devices, but the embodiment is not so limited.

The gateway of an alternative embodiment communicates over a wired physical coupling or connection to the security panel using the panel's specific wired hardware (bus) interface and the panel's bus-level protocol.

In an alternative embodiment, the Touchscreen **1203** implements the same PanelConnect API **1214** locally on the Touchscreen **1203**, communicating directly with the Security Panel **2** and/or Sensors **2** over the proprietary RF link or over a wired link for that system. In this embodiment the Touchscreen **1203**, instead of the gateway **1202**, incorporates the 345 MHz RF transceiver to communicate directly with Security Panel **2** or Sensors **2** over the RF link **2**. In the case of a wired link the Touchscreen **1203** incorporates the real-time hardware (e.g. a PIC chip and RS232-variant serial link) to physically connect to and satisfy the specific bus-level timing requirements of the SecurityPanel**2**.

In yet another alternative embodiment, either the gateway **1202** or the Touchscreen **1203** implements the remote service APIs. This embodiment includes a Cricket device ("Cricket") which comprises but is not limited to the following components: a processor (suitable for handling 802.11 protocols and processing, as well as the bus timing requirements of SecurityPanel**1**); an 802.11 (WiFi) client IP interface chip; and, a serial bus interface chip that implements variants of RS232 or RS485, depending on the specific Security Panel.

The Cricket also implements the full PanelConnect APIs such that it can perform the same functions as the case where the gateway implements the PanelConnect APIs. In this embodiment, the touchscreen core application **1210** calls functions in the remote service APIs **1212** (such as setArmState( ). These functions in turn couple or connect to the remote Cricket through a standard IP connection ("Cricket IP Link") (e.g., Ethernet, Homeplug, the gateway's proprietary Wifi network, etc.). The Cricket in turn implements the PanelConnect API, which responds to the request from the touchscreen core application, and performs the appropriate function using the proprietary panel interface. This interface uses either the wireless or wired proprietary protocol for the specific security panel and/or sensors.

An example use case that illustrates the use of the touchscreen embodiments described above is a panic alarm. FIG. **13** is a data flow diagram for a panic alarm **1300**, under an embodiment. In order to activate a panic alarm on the touchscreen, the user presses one of the panic alarm buttons, and confirms the alarm with a second button press (Step **1**). When the alarm is activated, in Step **2** the touchscreen sends the alarm signal to both the security panel and the gateway (using the PanelConnect or remote Svc API interface described above).

In Step **3**, the security panel alerts other keypads and touchscreens (once again through the PanelConnect interface) of the alarm condition, and flashes lights/sounds sirens as appropriate. The gateway or security panel calls the CMS on the hard-wired phone line. Simultaneously, the gateway sends a signal to the iConnect Server system over the broadband connection and, if so configured, uses GPRS to call a cell phone relay station with the alarm data. In Step **4**, the iConnect Server system routes the information, formatted using an industry standard alarm format such as ContactID or SIA, to a suitable broadband receiver in the CMS (for example the DSC Surguard broadband alarm receiver, or directly to the CMS automation software server). At the same time, in Step **5** the server system will also call a phone, send an SMS message, or send an email to any designated receiver.

The second example use case involving the touchscreen is a device installation example. FIG. **14** is a data flow diagram for device installation **1400**, under an embodiment. To make installation easier, the user can receive feedback from the touchscreen about what devices have been programmed in to the system, and the system automatically couples or connects to the CMS to configure the sensors on the back end.

As a data flow, in Step **1** the installer initiates entry into sensor learning mode by activating the installation UI on the touchscreen. When the installer triggers or otherwise activates a sensor in Step **2**, the gateway picks up the wireless communication from the sensor and pushes information about the sensor to the touchscreen (Step **3**). At this point, the installer can program the specific name of the sensor and its zones. This process is repeated for all of the sensors in the system. Once all sensors have been 'learned' in this way, the information is transmitted via internet or cellular IP networks to the iConnect server. The sensor information is associated with a 'network' (e.g., a location), but has not yet been associated with a specific user or account. After this step, the installer then creates a user account, and the previously created network is then associated with that account in the iConnect user database. This embodiment allows systems, devices, touchscreens, panels, and the like to be pre-associated, packaged, and/or installed without reference to a user or subscriber account.

To ensure that the security system is operating properly, it is next put into test mode. As the installer opens and closes the sensor, the touchscreen places a 'check' next to the name of the sensor. At the same time, in Step **4** the gateway pushes the open/close information to the iConnect servers, which alert the CMS to verify that a signal has been received for the sensor on the back end. In Step **5**, the CMS acknowledges that the sensor has been installed correctly and is operational, and that acknowledgement is pushed back through the system. When the system installation is finished, the iConnect servers send a notification of the installation, along with sensor set up information, and electronic verification of the test process for all sensors to the service provider.

Yet another example use case involving the touchscreen is a camera event. FIG. **15** is a data flow diagram for a camera event **1500**, under an embodiment. Cameras can be integrated with alerts that are generated by sensor events. For example, a consumer who wishes to see who is at her front door would set up the front door sensor to trigger an iControl Notification to the touchscreen, signifying a camera alert. When the sensor is activated, a pop-up appears on the touchscreen telling the user that the front door sensor has been activated, and asking the user if he or she would like to view the video.

The flow diagram for the camera event **1500** shows the flow of data from the sensor to the security panel and the gateway during a camera event. The gateway receives information regarding automation 'rules' between camera and sensor event from the iConnect servers as a part of the periodic state updates that occur between gateway client and server.

In Step **1** a sensor or multiple sensors are triggered. In Step **2** the gateway and/or Security Panel receives notification that a sensor state has changed through a network connection (wired or wireless) with the sensor, and if a rule exists for that device or set of devices, the touchscreen is then alerted via the PanelConnect interface running either locally on the touchscreen or remotely on the gateway. In Step **3**, the touchscreen puts up the alert and, if requested, opens a video stream from the camera. In the event that the touchscreen is in a quiescent mode instead of a dialog popup the IP video is immediately displayed, and an audible alert may sound as an option in the notification.

Step **3** of the data flow also shows an alternate route over which the gateway, if so configured, can send the sensor information the iControl servers (Step **4**), which in turn forward the information in the form of an SMS alert or direct IP notification to a cell phone (Step **5**). The cell phone user could then set up a video stream from the camera.

FIG. **16** is a flow diagram of a method of integrating an external control and management application system with an existing security system, under an embodiment. Operations begin when the system is powered on **1610**, involving at a minimum the power-on of the gateway device, and optionally the power-on of the connection between the gateway device and the remote servers. The gateway device initiates **1620** a software and RF sequence to locate the extant security system. The gateway and installer initiate and complete **1630** a sequence to 'learn' the gateway into the security system as a valid and authorized control device. The gateway initiates **1640** another software and RF sequence of instructions to discover and learn the existence and capabilities of existing RF devices within the extant security system, and store this information in the system. These operations under the system of an embodiment are described in further detail below.

Unlike conventional systems that extend an existing security system, the system of an embodiment operates utilizing the proprietary wireless protocols of the security system manufacturer. In one illustrative embodiment, the gateway is an embedded computer with an IP LAN and WAN connection and a plurality of RF transceivers and software protocol modules capable of communicating with a plurality of security systems each with a potentially different RF and software protocol interface. After the gateway has completed the discovery and learning **1640** of sensors and has been integrated **1650** as a virtual control device in the extant security system, the system becomes operational. Thus, the security system and associated sensors are presented **1650** as accessible devices to a potential plurality of user interface subsystems.

The system of an embodiment integrates **1660** the functionality of the extant security system with other non-security devices including but not limited to IP cameras, touchscreens, lighting controls, door locking mechanisms, which may be controlled via RF, wired, or powerline-based networking mechanisms supported by the gateway or servers.

The system of an embodiment provides a user interface subsystem **1670** enabling a user to monitor, manage, and control the system and associated sensors and security systems. In an embodiment of the system, a user interface subsystem is an HTML/XML/Javascript/Java/AJAX/Flash presentation of a monitoring and control application, enabling users to view the state of all sensors and controllers in the extant security system from a web browser or equivalent operating on a computer, PDA, mobile phone, or other consumer device.

In another illustrative embodiment of the system described herein, a user interface subsystem is an HTML/XML/Javascript/Java/AJAX presentation of a monitoring and control application, enabling users to combine the monitoring and control of the extant security system and sensors with the monitoring and control of non-security devices including but not limited to IP cameras, touchscreens, lighting controls, door locking mechanisms.

In another illustrative embodiment of the system described herein, a user interface subsystem is a mobile phone application enabling users to monitor and control the extant security system as well as other non-security devices.

In another illustrative embodiment of the system described herein, a user interface subsystem is an application running on a keypad or touchscreen device enabling users to monitor and control the extant security system as well as other non-security devices.

In another illustrative embodiment of the system described herein, a user interface subsystem is an application operating on a TV or set-top box connected to a TV enabling users to monitor and control the extant security system as well as other non-security devices.

FIG. **17** is a block diagram of an integrated security system **1700** wirelessly interfacing to proprietary security systems, under an embodiment. A security system **1710** is coupled or connected to a Gateway **1720**, and from Gateway **1720** coupled or connected to a plurality of information and content sources across a network **1730** including one or more web servers **1740**, system databases **1750**, and applications servers **1760**. While in one embodiment network **1730** is the Internet, including the World Wide Web, those of skill in the art will appreciate that network **1730** may be any type of network, such as an intranet, an extranet, a virtual private network (VPN), a mobile network, or a non-TCP/IP based network.

Moreover, other elements of the system of an embodiment may be conventional, well-known elements that need not be explained in detail herein. For example, security system **1710** could be any type home or business security system, such devices including but not limited to a standalone RF home security system or a non-RF-capable wired home security system with an add-on RF interface module. In the integrated security system **1700** of this example, security system **1710** includes an RF-capable wireless security panel (WSP) **1711** that acts as the master controller for security system **1710**. Well-known examples of such a WSP include the GE Security Concord, Networx, and Simon panels, the Honeywell Vista and Lynx panels, and similar panesl from DSC and Napco, to name a few. A wireless module **1714** includes the RF hardware and protocol software necessary to enable communication with and control of a plurality of wireless devices **1713**. WSP **1711** may also manage wired devices **1714** physically connected to WSP **1711** with an RS232 or RS485 or Ethernet connection or similar such wired interface.

In an implementation consistent with the systems and methods described herein, Gateway **1720** provides the interface between security system **1710** and LAN and/or WAN for purposes of remote control, monitoring, and management. Gateway **1720** communicates with an external web server **1740**, database **1750**, and application server **1760** over network **1730** (which may comprise WAN, LAN, or a combination thereof). In this example system, application logic, remote user interface functionality, as well as user state and account are managed by the combination of these remote servers. Gateway **1720** includes server connection manager **1721**, a software interface module responsible for all server communication over network **1730**. Event manager **1722** implements the main event loop for Gateway **1720**, processing events received from device manager **1724** (communicating with non-security system devices including but not limited to IP cameras, wireless thermostats, or remote door locks). Event manager **1722** further processes events and control messages from and to security system **1710** by utilizing WSP manager **1723**.

WSP manager **1723** and device manager **1724** both rely upon wireless protocol manager **1726** which receives and stores the proprietary or standards-based protocols required to support security system **1710** as well as any other devices interfacing with gateway **1720**. WSP manager **1723** further utilizes the comprehensive protocols and interface algorithms for a plurality of security systems **1710** stored in the WSP DB client database associated with wireless protocol manager **1726**. These various components implement the software logic and protocols necessary to communicate with and manager devices and security systems **1710**. Wireless Transceiver hardware modules **1725** are then used to implement the physical RF communications link to such devices and security systems **1710**. An illustrative wireless transceiver **1725** is the GE Security Dialog circuit board, implementing a 319.5 MHz two-way RF transceiver module. In this example, RF Link **1770** represents the 319.5 MHz RF communication link, enabling gateway **1720** to monitor and control WSP **1711** and associated wireless and wired devices **1713** and **1714**, respectively.

In one embodiment, server connection manager **1721** requests and receives a set of wireless protocols for a specific security system **1710** (an illustrative example being that of the GE Security Concord panel and sensors) and stores them in the WSP DB portion of the wireless protocol manager **1726**. WSP manager **1723** then utilizes such protocols from wireless protocol manager **1726** to initiate the sequence of processes detailed in FIG. **16** and FIG. **17** for learning gateway **1720** into security system **1710** as an authorized control device. Once learned in, as described with reference to FIG. **17** (and above), event manager **1722** processes all events and messages detected by the combination of WSP manager **1723** and the GE Security wireless transceiver module **1725**.

In another embodiment, gateway **1720** incorporates a plurality of wireless transceivers **1725** and associated protocols managed by wireless protocol manager **1726**. In this embodiment events and control of multiple heterogeneous devices may be coordinated with WSP **1711**, wireless devices **1713**, and wired devices **1714**. For example a wireless sensor from one manufacturer may be utilized to control a device using a different protocol from a different manufacturer.

In another embodiment, gateway **1720** incorporates a wired interface to security system **1710**, and incorporates a plurality of wireless transceivers **1725** and associated protocols managed by wireless protocol manager **1726**. In this embodiment events and control of multiple heterogeneous devices may be coordinated with WSP **1711**, wireless devices **1713**, and wired devices **1714**.

Of course, while an illustrative embodiment of an architecture of the system of an embodiment is described in detail herein with respect to FIG. **17**, one of skill in the art will understand that modifications to this architecture may be made without departing from the scope of the description presented herein. For example, the functionality described herein may be allocated differently between client and server, or amongst different server or processor-based components. Likewise, the entire functionality of the gateway **1720** described herein could be integrated completely within an existing security system **1710**. In such an embodiment, the architecture could be directly integrated with a security system **1710** in a manner consistent with the currently described embodiments.

FIG. **18** is a flow diagram for wirelessly 'learning' the Gateway into an existing security system and discovering extant sensors, under an embodiment. The learning interfaces gateway **1720** with security system **1710**. Gateway **1720** powers up **1810** and initiates software sequences **1820** and **1825** to identify accessible WSPs **1711** and wireless devices **1713**, respectively (e.g., one or more WSPs and/or devices within range of gateway **1720**). Once identified, WSP **1711** is manually or automatically set into 'learn mode' **1830**, and gateway **1720** utilizes available protocols to add **1840** itself as an authorized control device in security system **1710**. Upon successful completion of this task, WSP **1711** is manually or automatically removed from 'learn mode' **1850**.

Gateway **1720** utilizes the appropriate protocols to mimic **1860** the first identified device **1714**. In this operation gateway **1720** identifies itself using the unique or pseudo-unique identifier of the first found device **1714**, and sends an appropriate change of state message over RF Link **1770**. In the event that WSP **1711** responds to this change of state message, the device **1714** is then added **1870** to the system in database **1750**. Gateway **1720** associates **1880** any other information (such as zone name or token-based identifier) with this device **1714** in database **1750**, enabling gateway **1720**, user interface modules, or any application to retrieve this associated information.

In the event that WSP **1711** does not respond to the change of state message, the device **1714** is not added **1870** to the system in database **1750**, and this device **1714** is identified as not being a part of security system **1710** with a flag, and is either ignored or added as an independent device, at the discretion of the system provisioning rules. Operations hereunder repeat **1885** operations **1860**, **1870**, **1880** for all devices **1714** if applicable. Once all devices **1714** have been tested in this way, the system begins operation **1890**.

In another embodiment, gateway **1720** utilizes a wired connection to WSP **1711**, but also incorporates a wireless transceiver **1725** to communicate directly with devices **1714**. In this embodiment, operations under **1820** above are removed, and operations under **1840** above are modified so the system of this embodiment utilizes wireline protocols to add itself as an authorized control device in security system **1710**.

A description of an example embodiment follows in which the Gateway (FIG. **17**, element **1720**) is the iHub available from iControl Networks, Palo Alto, Calif., and described in detail herein. In this example the gateway is "automatically" installed with a security system.

The automatic security system installation begins with the assignment of an authorization key to components of the security system (e.g., gateway, kit including the gateway, etc.). The assignment of an authorization key is done in lieu of creating a user account. An installer later places the gateway in a user's premises along with the premises security system. The installer uses a computer to navigate to a web portal (e.g., integrated security system web interface), logs in to the portal, and enters the authorization key of the installed gateway into the web portal for authentication. Once authenticated, the gateway automatically discovers devices at the premises (e.g., sensors, cameras, light controls, etc.) and adds the discovered devices to the system or "network". The installer assigns names to the devices, and tests operation of the devices back to the server (e.g., did the door open, did the camera take a picture, etc.). The security device information is optionally pushed or otherwise propagated to a security panel and/or to the server network database. The installer finishes the installation, and instructs the end user on how to create an account, username, and password. At this time the user enters the authorization key which validates the account creation (uses a valid authorization key to associate the network with the user's account). New devices may subsequently be added to the security network in a variety of ways (e.g., user first enters a unique ID for each device/sensor and names it in the server, after which the gateway can automatically discover and configure the device).

A description of another example embodiment follows in which the security system (FIG. **17**, element **1710**) is a Dialog system and the WSP (FIG. **17**, element **1711**) is a SimonXT available from General Electric Security, and the Gateway (FIG. **17**, element **1720**) is the iHub available from iControl Networks, Palo Alto, Calif., and described in detail herein. Descriptions of the install process for the SimonXT and iHub are also provided below.

GE Security's Dialog network is one of the most widely deployed and tested wireless security systems in the world. The physical RF network is based on a 319.5 MHz unlicensed spectrum, with a bandwidth supporting up to 19 Kbps communications. Typical use of this bandwidth—even in conjunction with the integrated security system—is far less than that. Devices on this network can support either one-way communication (either a transmitter or a receiver) or two-way communication (a transceiver). Certain GE Simon, Simon XT, and Concord security control panels incorporate a two-way transceiver as a standard component. The gateway also incorporates the same two-way transceiver card. The physical link layer of the network is managed by the transceiver module hardware and firmware, while the coded payload bitstreams are made available to the application layer for processing.

Sensors in the Dialog network typically use a 60-bit protocol for communicating with the security panel transceiver, while security system keypads and the gateway use the encrypted 80-bit protocol. The Dialog network is configured for reliability, as well as low-power usage. Many devices are supervised, i.e. they are regularly monitored by the system 'master' (typically a GE security panel), while still maintaining excellent power usage characteristics. A typical door window sensor has a battery life in excess of 5-7 years.

The gateway has two modes of operation in the Dialog network: a first mode of operation is when the gateway is configured or operates as a 'slave' to the GE security panel; a second mode of operation is when the gateway is configured or operates as a 'master' to the system in the event a security panel is not present. In both configurations, the gateway has the ability to 'listen' to network traffic, enabling the gateway to continually keep track of the status of all devices in the system. Similarly, in both situations the gateway can address and control devices that support setting adjustments (such as the GE wireless thermostat).

In the configuration in which the gateway acts as a 'slave' to the security panel, the gateway is 'learned into' the system as a GE wireless keypad. In this mode of operation, the gateway emulates a security system keypad when managing the security panel, and can query the security panel for status and 'listen' to security panel events (such as alarm events).

The gateway incorporates an RF Transceiver manufactured by GE Security, but is not so limited. This transceiver implements the Dialog protocols and handles all network message transmissions, receptions, and timing. As such, the physical, link, and protocol layers of the communications between the gateway and any GE device in the Dialog network are totally compliant with GE Security specifications.

At the application level, the gateway emulates the behavior of a GE wireless keypad utilizing the GE Security 80-bit encrypted protocol, and only supported protocols and network traffic are generated by the gateway. Extensions to the Dialog RF protocol of an embodiment enable full control and configuration of the panel, and iControl can both automate installation and sensor enrollment as well as direct configuration downloads for the panel under these protocol extensions.

As described above, the gateway participates in the GE Security network at the customer premises. Because the gateway has intelligence and a two-way transceiver, it can 'hear' all of the traffic on that network. The gateway makes use of the periodic sensor updates, state changes, and supervisory signals of the network to maintain a current state of the premises. This data is relayed to the integrated security system server (e.g., FIG. **2**, element **260**) and stored in the event repository for use by other server components. This usage of the GE Security RF network is completely non-invasive; there is no new data traffic created to support this activity.

The gateway can directly (or indirectly through the Simon XT panel) control two-way devices on the network. For example, the gateway can direct a GE Security Thermostat to change its setting to 'Cool' from 'Off', as well as request an update on the current temperature of the room. The gateway performs these functions using the existing GE Dialog protocols, with little to no impact on the network; a gateway device control or data request takes only a few dozen bytes of data in a network that can support 19 Kbps.

By enrolling with the Simon XT as a wireless keypad, as described herein, the gateway includes data or information of all alarm events, as well as state changes relevant to the security panel. This information is transferred to the gateway as encrypted packets in the same way that the information is transferred to all other wireless keypads on the network.

Because of its status as an authorized keypad, the gateway can also initiate the same panel commands that a keypad can initiate. For example, the gateway can arm or disarm the panel using the standard Dialog protocol for this activity. Other than the monitoring of standard alarm events like other network keypads, the only incremental data traffic on the network as a result of the gateway is the infrequent remote arm/disarm events that the gateway initiates, or infrequent queries on the state of the panel.

The gateway is enrolled into the Simon XT panel as a 'slave' device which, in an embodiment, is a wireless keypad. This enables the gateway for all necessary functionality for operating the Simon XT system remotely, as well as combining the actions and information of non-security devices such as lighting or door locks with GE Security devices. The only resource taken up by the gateway in this scenario is one wireless zone (sensor ID).

The gateway of an embodiment supports three forms of sensor and panel enrollment/installation into the integrated security system, but is not limited to this number of enrollment/installation options. The enrollment/installation options of an embodiment include installer installation, kitting, and panel, each of which is described below.

Under the installer option, the installer enters the sensor IDs at time of installation into the integrated security system web portal or iScreen. This technique is supported in all configurations and installations.

Kits can be pre-provisioned using integrated security system provisioning applications when using the kitting option. At kitting time, multiple sensors are automatically associated with an account, and at install time there is no additional work required.

In the case where a panel is installed with sensors already enrolled (i.e. using the GE Simon XT enrollment process), the gateway has the capability to automatically extract the sensor information from the system and incorporate it into the user account on the integrated security system server.

The gateway and integrated security system of an embodiment uses an auto-learn process for sensor and panel enrollment in an embodiment. The deployment approach of an embodiment can use additional interfaces that GE Security is adding to the Simon XT panel. With these interfaces, the gateway has the capability to remotely enroll sensors in the panel automatically. The interfaces include, but are not limited to, the following: EnrollDevice(ID, type, name, zone, group); SetDeviceParameters(ID, type, Name, zone, group), GetDeviceParameters(zone); and RemoveDevice(zone).

The integrated security system incorporates these new interfaces into the system, providing the following install process. The install process can include integrated security system logistics to handle kitting and pre-provisioning. Pre-kitting and logistics can include a pre-provisioning kitting tool provided by integrated security system that enables a security system vendor or provider ("provider") to offer pre-packaged initial 'kits'. This is not required but is recommended for simplifying the install process. This example assumes a 'Basic' kit is preassembled and includes one (1) Simon XT, three (3) Door/window sensors, one (1) motion sensor, one (1) gateway, one (1) keyfob, two (2) cameras, and ethernet cables. The kit also includes a sticker page with all Zones (**1**-**2**) and Names (full name list).

The provider uses the integrated security system kitting tool to assemble 'Basic' kit packages. The contents of different types of starter kits may be defined by the provider. At the distribution warehouse, a worker uses a bar code scanner to scan each sensor and the gateway as it is packed into the box. An ID label is created that is attached to the box. The scanning process automatically associates all the devices with one kit, and the new ID label is the unique identifier of the kit. These boxes are then sent to the provider for distribution to installer warehouses. Individual sensors, cameras, etc. are also sent to the provider installer warehouse. Each is labeled with its own barcode/ID.

An installation and enrollment procedure of a security system including a gateway is described below as one example of the installation process.

1. Order and Physical Install Process
    a. Once an order is generated in the iControl system, an account is created and an install ticket is created and sent electronically to the provider for assignment to an installer.
    b. The assigned installer picks up his/her ticket(s) and fills his/her truck with Basic and/or Advanced starter kits. He/she also keeps a stock of individual sensors, cameras, iHubs, Simon XTs, etc. Optionally, the installer can also stock homeplug adapters for problematic installations.
    c. The installer arrives at the address on the ticket, and pulls out the Basic kit. The installer determines sensor locations from a tour of the premises and discussion with the homeowner. At this point assume the homeowner requests additional equipment including an extra camera, two (2) additional door/window sensors, one (1) glass break detector, and one (1) smoke detector.
    d. Installer mounts SimonXT in the kitchen or other location in the home as directed by the homeowner, and routes the phone line to Simon XT if available. GPRS and Phone numbers pre-programmed in SimonXT to point to the provider Central Monitoring Station (CMS).
    e. Installer places gateway in the home in the vicinity of a router and cable modem. Installer installs an ethernet line from gateway to router and plugs gateway into an electrical outlet.
2. Associate and Enroll gateway into SimonXT
    a. Installer uses either his/her own laptop plugged into router, or homeowners computer to go to the integrated security system web interface and log in with installer ID/pass.
    b. Installer enters ticket number into admin interface, and clicks 'New Install' button. Screen prompts installer for kit ID (on box's barcode label).
    c. Installer clicks 'Add SimonXT'. Instructions prompt installer to put Simon XT into install mode, and add gateway as a wireless keypad. It is noted that this step is for security only and can be automated in an embodiment.
    d. Installer enters the installer code into the Simon XT. Installer Learns 'gateway' into the panel as a wireless keypad as a group **1** device.
    e. Installer goes back to Web portal, and clicks the 'Finished Adding SimonXT' button.
3. Enroll Sensors into SimonXT via iControl
    a. All devices in the Basic kit are already associated with the user's account.
    b. For additional devices, Installer clicks 'Add Device' and adds the additional camera to the user's account (by typing in the camera ID/Serial #).
    c. Installer clicks 'Add Device' and adds other sensors (two (2) door/window sensors, one (1) glass break sensor, and one (1) smoke sensor) to the account (e.g., by typing in IDs).

d. As part of Add Device, Installer assigns zone, name, and group to the sensor. Installer puts appropriate Zone and Name sticker on the sensor temporarily.
e. All sensor information for the account is pushed or otherwise propagated to the iConnect server, and is available to propagate to CMS automation software through the CMS application programming interface (API).
f. Web interface displays 'Installing Sensors in System . . . ' and automatically adds all of the sensors to the Simon XT panel through the GE RF link.
g. Web interface displays 'Done Installing'—>all sensors show green.
4. Place and Tests Sensors in Home
a. Installer physically mounts each sensor in its desired location, and removes the stickers.
b. Installer physically mounts WiFi cameras in their location and plugs into AC power. Optional fishing of low voltage wire through wall to remove dangling wires. Camera transformer is still plugged into outlet but wire is now inside the wall.
c. Installer goes to Web interface and is prompted for automatic camera install. Each camera is provisioned as a private, encrypted Wifi device on the gateway secured sandbox network, and firewall NAT traversal is initiated. Upon completion the customer is prompted to test the security system.
d. Installer selects the 'Test System' button on the web portal—the SimonXT is put into Test mode by the gateway over GE RF.
e. Installer manually tests the operation of each sensor, receiving an audible confirmation from SimonXT.
f. gateway sends test data directly to CMS over broadband link, as well as storing the test data in the user's account for subsequent report generation.
g. Installer exits test mode from the Web portal.
5. Installer instructs customer on use of the Simon XT, and shows customer how to log into the iControl web and mobile portals. Customer creates a username/password at this time.
6. Installer instructs customer how to change Simon XT user code from the Web interface. Customer changes user code which is pushed to SimonXT automatically over GE RE.

An installation and enrollment procedure of a security system including a gateway is described below as an alternative example of the installation process. This installation process is for use for enrolling sensors into the SimonXT and integrated security system and is compatible with all existing GE Simon panels.

The integrated security system supports all pre-kitting functionality described in the installation process above. However, for the purpose of the following example, no kitting is used.

1. Order and Physical Install Process
a. Once an order is generated in the iControl system, an account is created and an install ticket is created and sent electronically to the security system provider for assignment to an installer.
b. The assigned installer picks up his/her ticket(s) and fills his/her truck with individual sensors, cameras, iHubs, Simon XTs, etc. Optionally, the installer can also stock homeplug adapters for problematic installations.
c. The installer arrives at the address on the ticket, and analyzes the house and talks with the homeowner to determine sensor locations. At this point assume the homeowner requests three (3) cameras, five (5) door/window sensors, one (1) glass break detector, one (1) smoke detector, and one (1) keyfob.
d. Installer mounts SimonXT in the kitchen or other location in the home. The installer routes a phone line to Simon XT if available. GPRS and Phone numbers are pre-programmed in SimonXT to point to the provider CMS.
e. Installer places gateway in home in the vicinity of a router and cable modem, and installs an ethernet line from gateway to the router, and plugs gateway into an electrical outlet.
2. Associate and Enroll gateway into SimonXT
a. Installer uses either his/her own laptop plugged into router, or homeowners computer to go to the integrated security system web interface and log in with an installer ID/pass.
b. Installer enters ticket number into admin interface, and clicks 'New Install' button. Screen prompts installer to add devices.
c. Installer types in ID of gateway, and it is associated with the user's account.
d. Installer clicks 'Add Device' and adds the cameras to the user's account (by typing in the camera ID/Serial #).
e. Installer clicks 'Add SimonXT'. Instructions prompt installer to put Simon XT into install mode, and add gateway as a wireless keypad.
f. Installer goes to Simon XT and enters the installer code into the Simon XT. Learns 'gateway' into the panel as a wireless keypad as group **1** type sensor.
g. Installer returns to Web portal, and clicks the 'Finished Adding SimonXT' button.
h. Gateway now is alerted to all subsequent installs over the security system RF.
3. Enroll Sensors into SimonXT via iControl
a. Installer clicks 'Add Simon XT Sensors'—Displays instructions for adding sensors to Simon XT.
b. Installer goes to Simon XT and uses Simon XT install process to add each sensor, assigning zone, name, group. These assignments are recorded for later use.
c. The gateway automatically detects each sensor addition and adds the new sensor to the integrated security system.
d. Installer exits install mode on the Simon XT, and returns to the Web portal.
e. Installer clicks 'Done Adding Devices'.
f. Installer enters zone/sensor naming from recorded notes into integrated security system to associate sensors to friendly names.
g. All sensor information for the account is pushed to the iConnect server, and is available to propagate to CMS automation software through the CMS API.
4. Place and Tests Sensors in Home
a. Installer physically mounts each sensor in its desired location.
b. Installer physically mounts Wifi cameras in their location and plugs into AC power. Optional fishing of low voltage wire through wall to remove dangling wires. Camera transformer is still plugged into outlet but wire is now inside the wall.
c. Installer puts SimonXT into Test mode from the keypad.
d. Installer manually tests the operation of each sensor, receiving an audible confirmation from SimonXT.
e. Installer exits test mode from the Simon XT keypad.

f. Installer returns to web interface and is prompted to automatically set up cameras. After waiting for completion cameras are now provisioned and operational.

5. Installer instructs customer on use of the Simon XT, and shows customer how to log into the integrated security system web and mobile portals. Customer creates a username/password at this time.
6. Customer and Installer observe that all sensors/cameras are green.
7. Installer instructs customer how to change Simon XT user code from the keypad. Customer changes user code and stores in SimonXT.
8. The first time the customer uses the web portal to Arm/Disarm system the web interface prompts the customer for the user code, which is then stored securely on the server. In the event the user code is changed on the panel the web interface once again prompts the customer.

The panel of an embodiment can be programmed remotely. The CMS pushes new programming to SimonXT over a telephone or GPRS link. Optionally, iControl and GE provide a broadband link or coupling to the gateway and then a link from the gateway to the Simon XT over GE RF.

As described above, computer networks suitable for use with the embodiments described herein include local area networks (LAN), wide area networks (WAN), Internet, or other connection services and network variations such as the world wide web, the public internet, a private internet, a private computer network, a public network, a mobile network, a cellular network, a value-added network, and the like. Computing devices coupled or connected to the network may be any microprocessor controlled device that permits access to the network, including terminal devices, such as personal computers, workstations, servers, mini computers, mainframe computers, laptop computers, mobile computers, palm top computers, hand held computers, mobile phones, TV set-top boxes, or combinations thereof. The computer network may include one of more LANs, WANs, Internets, and computers. The computers may serve as servers, clients, or a combination thereof.

The integrated security system can be a component of a single system, multiple systems, and/or geographically separate systems. The integrated security system can also be a subcomponent or subsystem of a single system, multiple systems, and/or geographically separate systems. The integrated security system can be coupled to one or more other components (not shown) of a host system or a system coupled to the host system.

One or more components of the integrated security system and/or a corresponding system or application to which the integrated security system is coupled or connected includes and/or runs under and/or in association with a processing system. The processing system includes any collection of processor-based devices or computing devices operating together, or components of processing systems or devices, as is known in the art. For example, the processing system can include one or more of a portable computer, portable communication device operating in a communication network, and/or a network server. The portable computer can be any of a number and/or combination of devices selected from among personal computers, personal digital assistants, portable computing devices, and portable communication devices, but is not so limited. The processing system can include components within a larger computer system.

The processing system of an embodiment includes at least one processor and at least one memory device or subsystem. The processing system can also include or be coupled to at least one database. The term "processor" as generally used herein refers to any logic processing unit, such as one or more central processing units (CPUs), digital signal processors (DSPs), application-specific integrated circuits (ASIC), etc. The processor and memory can be monolithically integrated onto a single chip, distributed among a number of chips or components, and/or provided by some combination of algorithms. The methods described herein can be implemented in one or more of software algorithm(s), programs, firmware, hardware, components, circuitry, in any combination.

The components of any system that includes the integrated security system can be located together or in separate locations. Communication paths couple the components and include any medium for communicating or transferring files among the components. The communication paths include wireless connections, wired connections, and hybrid wireless/wired connections. The communication paths also include couplings or connections to networks including local area networks (LANs), metropolitan area networks (MANs), wide area networks (WANs), proprietary networks, interoffice or backend networks, and the Internet. Furthermore, the communication paths include removable fixed mediums like floppy disks, hard disk drives, and CD-ROM disks, as well as flash RAM, Universal Serial Bus (USB) connections, RS-232 connections, telephone lines, buses, and electronic mail messages.

Embodiments of the integrated security system include a device comprising: a touchscreen at a first location, wherein the touchscreen includes a processor coupled to a local area network (LAN) and a security system at the first location; and a plurality of interfaces coupled to the processor and presented to a user via the touchscreen, wherein the plurality of interfaces include a security interface and a network interface, wherein the security interface provides the user with control of functions of the security system and access to data collected by the security system, wherein the network interface allows the user to transfer content to and from a wide area network (WAN) coupled to the LAN; and a remote server coupled to the touchscreen, the remote server managing at least one of the touchscreen and the security system.

The remote server of an embodiment allows a user to configure content of the touchscreen.

The remote server of an embodiment provides user portals that enable content and information displayed on the touchscreen to be displayed on other devices.

The other devices of an embodiment include at least one of HTML browsers, WEB/WAP phones, and desktop widgets.

The security system of an embodiment is managed via applications entirely within the touchscreen.

The touchscreen of an embodiment includes a wireless transceiver for communicating with security system components of the security system.

The touchscreen of an embodiment plays live video from a camera, wherein the camera is an Internet Protocol (IP) camera.

The camera of an embodiment is at the first location.

The camera of an embodiment is at a second location managed by the remote server.

The live video of an embodiment is accessed through internet content widgets.

The live video of an embodiment is IP video.

The live video of an embodiment is MPEG-4 video.

The live video of an embodiment is Motion JPEG (MJPEG) video.

Devices of an embodiment are added to the security system through the touchscreen.

Devices of an embodiment are added to a user account on the remote server through the touchscreen.

Device information and device data of an embodiment are transmitted to from the devices to the remote server.

The device information of an embodiment includes at least one of device name and device type, wherein the device data includes at least one of device state and battery state.

Device information and device data of an embodiment are associated with a user account by the remote server.

The devices of an embodiment are automatically detected by the touchscreen and added to a user account on the remote server through the touchscreen.

The coupling with the LAN of an embodiment is over 802.11.

The touchscreen of an embodiment integrates the content with the access and control of the security system.

The content of an embodiment includes interactive content in the form of internet widgets.

The network interface of an embodiment allows the user to transfer at least one of content and internet widgets to and from the LAN.

The network interface of an embodiment allows the user to control functions of peripheral devices of the first location coupled to the LAN.

The plurality of interfaces of an embodiment are configurable.

The network interface of an embodiment provides the user with communication and control of a plurality of network devices coupled to the LAN.

The network interface of an embodiment provides the user with communication and control of a plurality of security system components, wherein the security system comprises the plurality of security system components.

The WAN of an embodiment is the internet and the network interface of an embodiment is a web browser.

The touchscreen of an embodiment integrates at least one of a security system control panel and an internet browser.

The device of an embodiment comprises an application engine coupled to the processor, wherein the application engine controls a plurality of applications executing under the processor.

The plurality of applications of an embodiment includes a security application and a content application, wherein the security application provides the security interface and the content application provides the network interface.

The plurality of applications of an embodiment provides interactivity with a plurality of devices via the plurality of interfaces.

The plurality of devices of an embodiment are coupled to the processor.

The plurality of devices of an embodiment are coupled to the processor via a wireless coupling.

The plurality of devices of an embodiment include a plurality of devices of the security system.

The plurality of devices of an embodiment include a plurality of devices of the LAN.

The plurality of devices of an embodiment include a plurality of devices of the WAN.

The plurality of applications of an embodiment are accessed and loaded directly via the WAN.

The touchscreen of an embodiment includes the plurality of applications.

The plurality of applications of an embodiment includes a resident application that manages interactions between the plurality of applications.

The resident application of an embodiment manages interactions between the plurality of devices.

The resident application of an embodiment determines a priority of each application of the plurality of applications and manages the plurality of applications according to the priority.

The resident application of an embodiment allows a first application having a first priority to override a second application having a second priority when the first priority is higher than the second priority.

The device of an embodiment comprises a first application engine coupled to the processor, wherein the first application engine executes a security application that provides the security interface. The device of an embodiment comprises a second application engine coupled to the processor, wherein the second application engine executes a content application that provides the network interface.

The device of an embodiment comprises a core engine coupled to the processor, the core engine controlling dynamic provisioning of the plurality of applications and the content.

The core engine of an embodiment manages images received from a plurality devices of at least one of the security system and the LAN.

The images of an embodiment include video.

The processor of an embodiment is coupled to the WAN via a broadband coupling.

The processor of an embodiment is coupled to the WAN via a cellular data coupling.

The plurality of interfaces of an embodiment provides interactivity with a plurality of devices via the plurality of interfaces.

A device of the plurality of devices of an embodiment is an Internet Protocol device.

A device of the plurality of devices of an embodiment is a camera.

A device of the plurality of devices of an embodiment is another touchscreen.

A device of the plurality of devices of an embodiment is a device controller that controls an attached device.

The device controller of an embodiment is a thermostat.

The device controller of an embodiment is an energy meter.

A device of the plurality of devices of an embodiment is a sensor.

The network interface of an embodiment allows a user to control functions of peripheral devices coupled to other touchscreens located at remote locations.

Embodiments of the integrated security system include a device comprising: a touchscreen at a first location, wherein the touchscreen includes a processor coupled to a local area network (LAN) and a security system at the first location; a plurality of applications coupled to the processor, the plurality of applications displaying a plurality of interfaces to a user via the touchscreen, the plurality of interfaces including a security interface and a network interface, wherein the security interface provides the user with control of functions of the security system and access to data collected by the security system, wherein the network interface allows the user to transfer content to and from a remote network coupled to the LAN; and a remote server coupled to the touchscreen, the remote server managing at least one of the touchscreen and the security system.

Embodiments of the integrated security system include a device comprising: an input/output (I/O) device at a first location, the I/O device comprising a processor coupled to a local area network (LAN) and a security system at the first location, wherein the security system includes a plurality of security system components that are proprietary to the security system; a security application coupled to the processor, the security application providing a security interface for control of functions of the security system, the security interface presented to a user via the I/O device; a content application coupled to a processor, the content application providing a network interface for access to networked content of a remote wide area network (WAN), the network interface presented to a user via the I/O device, wherein the I/O device is coupled to the WAN via the LAN; and a remote server coupled to the I/O device, the remote server managing at least one of the I/O device and the security system.

Embodiments of the integrated security system include a system comprising: a gateway at a first location, the gateway coupled to a local area network (LAN) and a security system of the first location, wherein the security system includes a plurality of security system components, the gateway forming a security network that integrates functions of the security system with the LAN; a touchscreen coupled to the gateway, the touchscreen including a plurality of interfaces presented to a user, wherein the plurality of interfaces include a security interface and a network interface, wherein the security interface provides interactivity with the security system, wherein the network interface provides interactivity with networked content of a remote network.

The system of an embodiment comprises a security server located at a second location different from the first location, the security server coupled to the gateway, the touchscreen providing interactivity with networked content of a remote network via the security server.

The security interface of an embodiment provides the user with control of functions of the security system and access to data collected by the security system

The network interface of an embodiment allows the user to transfer content to and from a wide area network (WAN) coupled to the LAN.

The gateway of an embodiment integrates the content with access and control of the security system.

The content of an embodiment includes interactive content.

The network interface of an embodiment allows the user to transfer content to and from the LAN.

The network interface of an embodiment allows the user to control functions of network devices of the first location coupled to the LAN.

The plurality of interfaces of an embodiment are configurable.

The network interface of an embodiment provides interactivity with a plurality of network devices coupled to the LAN.

The security interface of an embodiment provides the user with communication and control of the plurality of security system components.

The remote network of an embodiment is the internet and the network interface is a web browser.

The touchscreen of an embodiment integrates a security system control panel and an internet browser.

The system of an embodiment comprises an application engine coupled to the touchscreen, wherein the application engine controls a plurality of applications executing under the processor.

The plurality of applications of an embodiment includes a security application and a content application, wherein the security application provides the security interface and the content application provides the network interface.

The plurality of applications of an embodiment provides interactivity with a plurality of devices via the plurality of interfaces.

The plurality of devices of an embodiment are coupled to at least one of the touchscreen and the gateway.

The plurality of devices of an embodiment are coupled to at least one of the touchscreen and the gateway via a wireless coupling.

The plurality of devices of an embodiment include a plurality of devices of the security system.

The plurality of devices of an embodiment include a plurality of devices of the LAN.

The plurality of devices of an embodiment include a plurality of devices of the remote network.

The plurality of applications of an embodiment are accessed and loaded directly via the remote network.

The touchscreen of an embodiment includes the plurality of applications.

The plurality of applications of an embodiment includes a resident application that manages interactions between the plurality of applications.

The resident application of an embodiment manages interactions between a plurality of devices comprising at least one of the security system components, network devices coupled to the LAN, and devices coupled to the remote network.

The resident application of an embodiment determines a priority of each application of the plurality of applications and manages the plurality of applications according to the priority.

The resident application of an embodiment allows a first application having a first priority to override a second application having a second priority when the first priority is higher than the second priority.

The system of an embodiment comprises a first application engine coupled to the touchscreen, wherein the first application engine executes a security application that provides the security interface. The system of an embodiment comprises a second application engine coupled to the touchscreen, wherein the second application engine executes a content application that provides the network interface.

The system of an embodiment comprises a core engine coupled to the touchscreen, the core engine controlling dynamic provisioning of a plurality of applications and the content, the plurality of applications corresponding to the plurality of interfaces.

The core engine of an embodiment manages images received from a plurality devices of at least one of the security system and the LAN.

The images of an embodiment include video.

The touchscreen of an embodiment is coupled to the remote network via a broadband coupling.

The touchscreen of an embodiment is coupled to the remote network via a cellular coupling.

A plurality of applications of an embodiment provides interactivity with a plurality of devices via the plurality of interfaces.

A device of the plurality of devices of an embodiment is an Internet Protocol device.

A device of the plurality of devices of an embodiment is a camera.

A device of the plurality of devices of an embodiment is another touchscreen.

A device of the plurality of devices of an embodiment is a device controller that controls an attached device.

A device of the plurality of devices of an embodiment is a sensor.

The gateway of an embodiment is connected to the LAN at the first location, and the LAN is coupled to a wide area network via a router at the first location.

The gateway of an embodiment is coupled to a wide area network and is coupled to the LAN at the first location via a router at the first location.

The gateway of an embodiment is coupled to a security server via the internet, the security server located at a second location different from the first location, the touchscreen providing interactivity with networked content of a remote network via the security server.

The system of an embodiment comprises an interface coupled to the security network, wherein the interface allows control of the functions of the security network from remote client devices.

The remote client devices of an embodiment include one or more of personal computers, personal digital assistants, cellular telephones, and mobile computing devices.

The gateway of an embodiment automatically discovers the security system components.

The gateway of an embodiment uses protocols of the security system to discover the security system components.

The gateway of an embodiment automatically establishes a coupling with the security system including the security system components.

The gateway of an embodiment includes a rules component that manages rules of interaction between the gateway and the security system components.

The security system of an embodiment is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link, wherein the central monitoring station is located at a third location different from the first location and the second location.

The gateway of an embodiment transmits event data of the security system components to the central monitoring station over the secondary communication link.

The event data of an embodiment comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

The secondary communication link of an embodiment includes a broadband coupling.

The secondary communication link of an embodiment includes a cellular coupling.

The gateway of an embodiment transmits messages comprising event data of the security system components to remote client devices over the secondary communication link.

The event data of an embodiment comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

The gateway of an embodiment receives control data for control of the security system components from remote client devices via the secondary communication link.

The security network of an embodiment comprises network devices coupled to the gateway via a wireless coupling.

The gateway of an embodiment automatically discovers the network devices.

The gateway of an embodiment automatically installs the network devices in the security network.

The gateway of an embodiment automatically configures the network devices for operation in the security network.

The gateway of an embodiment controls communications between the network devices and the security system components.

The gateway of an embodiment transmits event data of the network devices to remote client devices over at least one of a plurality of communication links.

The gateway of an embodiment receives control data for control of the network devices from remote client devices via at least one of the plurality of communication links.

The event data of an embodiment comprises changes in device states of the network devices, data of the network devices, and data received by the network devices.

Embodiments of the integrated security system include a system comprising: a gateway at a first location, the gateway coupled to a local area network (LAN) and a security system of the first location, wherein the security system includes a plurality of security system components that are proprietary to the security system, the gateway forming a security network that integrates functions of the security system with the LAN; an input/output (I/O) device at the first location and coupled to the gateway, the I/O device providing control of functions of the security system and the LAN; and a security server located at a second location different from the first location, the security server coupled to the gateway, the I/O device providing interactivity with networked content of a remote network via the security server.

Embodiments of the integrated security system include a system comprising: a gateway at a first location, the gateway coupled to a security system of the first location, the security system including a plurality of security system components that are proprietary to the security system, the gateway forming a security network that integrates functions of the security system with network devices of a local area network (LAN) of the first location; a touchscreen coupled to the gateway at the first location, the touchscreen providing control of functions of the security system and the network devices; and a security server located at a second location different from the first location, the security server coupled to the gateway, the touchscreen providing interactivity with networked content of a remote network via the security server.

Embodiments of the integrated security system include a system comprising: a touchscreen at a first location, wherein the touchscreen includes a processor coupled to a local area network (LAN) and a security system at the first location; a plurality of interfaces coupled to the processor and presented to a user via the touchscreen, wherein the plurality of interfaces include a security interface and a network interface, wherein the security interface provides the user with control of functions of the security system and access to data collected by the security system, wherein the network interface allows the user to transfer content to and from a remote network coupled to the LAN; and a security server coupled to the touchscreen and the remote network, the security server located at a second location different from the first location.

The touchscreen of an embodiment provides interactivity with networked content of the remote network via the security server.

The touchscreen of an embodiment integrates the content with the access and the control of the security system.

The content of an embodiment includes interactive content.

The network interface of an embodiment allows the user to transfer content to and from the LAN.

The network interface of an embodiment allows the user to control functions of network devices coupled to the LAN.

The plurality of interfaces of an embodiment are configurable.

The network interface of an embodiment provides interactivity with a plurality of network devices coupled to the LAN.

The security system of an embodiment comprises a plurality of security system components, wherein the security interface provides the user with communication and control of the plurality of security system components.

The remote network of an embodiment is the internet and the network interface is a web browser.

The touchscreen of an embodiment integrates an internet browser and a security system control panel of the security system.

The system of an embodiment comprises an application engine coupled to the touchscreen, wherein the application engine controls a plurality of applications executing under the processor.

The plurality of applications of an embodiment includes a security application and a content application, wherein the security application provides the security interface and the content application provides the network interface.

The plurality of applications of an embodiment provides interactivity with a plurality of devices via the plurality of interfaces.

A plurality of devices of an embodiment are coupled to the touchscreen.

The plurality of devices of an embodiment are coupled to the touchscreen via a wireless coupling.

The plurality of devices of an embodiment include a plurality of devices of the security system.

The plurality of devices of an embodiment include a plurality of devices of the LAN.

The plurality of devices of an embodiment include a plurality of devices of the remote network.

The plurality of applications of an embodiment are accessed and loaded directly via the remote network.

The touchscreen of an embodiment includes the plurality of applications.

The plurality of applications of an embodiment includes a resident application that manages interactions between the plurality of applications.

The resident application of an embodiment manages interactions between a plurality of devices comprising at least one of the security system components, devices coupled to the LAN, and devices coupled to the remote network.

The resident application of an embodiment determines a priority of each application of the plurality of applications and manages the plurality of applications according to the priority.

The resident application of an embodiment allows a first application having a first priority to override a second application having a second priority when the first priority is higher than the second priority.

The system of an embodiment comprises a first application engine coupled to the touchscreen, wherein the first application engine executes a security application that provides the security interface. The system of an embodiment comprises a second application engine coupled to the touchscreen, wherein the second application engine executes a content application that provides the network interface.

The system of an embodiment comprises a core engine coupled to the touchscreen, the core engine controlling dynamic provisioning of a plurality of applications and the content, the plurality of applications corresponding to the plurality of interfaces.

The core engine of an embodiment manages images received from a plurality devices of at least one of the security system and the LAN.

The images of an embodiment include video.

The touchscreen of an embodiment is coupled to the remote network via a broadband coupling.

The touchscreen of an embodiment is coupled to the remote network via a cellular coupling.

A plurality of applications of an embodiment provides interactivity with a plurality of devices via the plurality of interfaces.

A device of the plurality of devices of an embodiment is an Internet Protocol device.

A device of the plurality of devices of an embodiment is a camera.

A device of the plurality of devices of an embodiment is another touchscreen.

A device of the plurality of devices of an embodiment is a device controller that controls an attached device.

A device of the plurality of devices of an embodiment is a sensor.

The touchscreen of an embodiment is connected to the LAN at the first location, and the LAN is coupled to a wide area network via a router at the first location.

The touchscreen of an embodiment is coupled to a wide area network and is coupled to the LAN at the first location via a router at the first location.

The gateway of an embodiment is coupled to the security server via the internet, the touchscreen providing interactivity with networked content of a remote network via the security server.

The system of an embodiment comprises a portal coupled to the security server, wherein the portal allows control of the functions of the security system from remote client devices.

The remote client devices of an embodiment include one or more of personal computers, personal digital assistants, cellular telephones, and mobile computing devices.

The touchscreen of an embodiment automatically discovers security system components of the security system.

The touchscreen of an embodiment uses protocols of the security system to discover the security system components.

The touchscreen of an embodiment automatically establishes a coupling with the security system.

The touchscreen of an embodiment includes a rules component that manages rules of interaction with the security system.

The security system of an embodiment is coupled to a central monitoring station via a primary communication link, wherein the security system comprises security system components, wherein the touchscreen is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link, wherein the central monitoring station is located at a third location different from the first location and the second location.

The touchscreen of an embodiment transmits event data of the security system to the central monitoring station over the secondary communication link.

The event data of an embodiment comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

The secondary communication link of an embodiment includes a broadband coupling.

The secondary communication link of an embodiment includes a cellular coupling.

The touchscreen of an embodiment transmits messages comprising event data of the security system components to remote client devices over the secondary communication link.

The event data of an embodiment comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

The touchscreen of an embodiment receives control data for control of the security system components from remote client devices via the secondary communication link.

Embodiments of the integrated security system include a system comprising: a touchscreen at a first location, wherein the touchscreen includes a processor coupled to a local area network (LAN) and a security system at the first location; a plurality of applications coupled to the processor, the plurality of applications displaying a plurality of interfaces to a user via the touchscreen, the plurality of interfaces including a security interface and a network interface, wherein the security interface provides the user with control of functions of the security system and access to data collected by the security system, wherein the network interface allows the user to transfer content to and from a remote network coupled to the LAN; and a security server coupled to the touchscreen and the remote network, the security server located at a second location different from the first location.

Embodiments of the integrated security system include a system comprising: an input/output (I/O) device at a first location, the I/O device comprising a processor coupled to a local area network (LAN) and a security system at the first location, wherein the security system includes a plurality of security system components that are proprietary to the security system; a security application coupled to the processor, the security application providing a security interface for control of functions of the security system, the security interface presented to a user via the I/O device; a content application coupled to a processor, the content application providing a network interface for access to networked content of a remote wide area network (WAN), the network interface presented to a user via the I/O device, wherein the I/O device is coupled to the WAN via the LAN; and a security server coupled to the I/O device and the WAN, the security server located at a second location different from the first location.

Embodiments of the integrated security system include a method comprising: coupling a touchscreen including a processor to a local area network (LAN) and a security system at a first location; and providing a plurality of interfaces to a user via the touchscreen, the plurality of interfaces coupled to the processor, wherein the plurality of interfaces include a security interface and a network interface, wherein the security interface provides the user with control of functions of the security system and access to data collected by the security system, wherein the network interface allows the user to transfer content to and from a wide area network (WAN) coupled to the LAN.

The touchscreen of an embodiment integrates the content with the access and control of the security system.

The content of an embodiment includes interactive content.

The network interface of an embodiment allows the user to transfer content to and from the LAN.

The network interface of an embodiment allows the user to control functions of peripheral devices of the first location coupled to the LAN.

The plurality of interfaces of an embodiment are configurable.

The network interface of an embodiment provides the user with communication and control of a plurality of network devices coupled to the LAN.

The network interface of an embodiment provides the user with communication and control of a plurality of security system components, wherein the security system comprises the plurality of security system components.

The WAN of an embodiment is the internet and the network interface of an embodiment is a web browser.

The touchscreen of an embodiment integrates a security system control panel and an internet browser.

The method of an embodiment comprises an application engine coupled to the processor, wherein the application engine controls a plurality of applications executing under the processor.

The plurality of applications of an embodiment includes a security application and a content application, wherein the security application provides the security interface and the content application provides the network interface.

The plurality of applications of an embodiment provides interactivity with a plurality of devices via the plurality of interfaces.

The plurality of devices of an embodiment are coupled to the processor.

The plurality of devices of an embodiment are coupled to the processor via a wireless coupling.

The plurality of devices of an embodiment include a plurality of devices of the security system.

The plurality of devices of an embodiment include a plurality of devices of the LAN.

The plurality of devices of an embodiment include a plurality of devices of the WAN.

The plurality of applications of an embodiment are accessed and loaded directly via the WAN.

The touchscreen of an embodiment includes the plurality of applications.

The plurality of applications of an embodiment includes a resident application that manages interactions between the plurality of applications.

The resident application of an embodiment manages interactions between the plurality of devices.

The resident application of an embodiment determines a priority of each application of the plurality of applications and manages the plurality of applications according to the priority.

The resident application of an embodiment allows a first application having a first priority to override a second application having a second priority when the first priority is higher than the second priority.

The method of an embodiment comprises a first application engine coupled to the processor, wherein the first application engine executes a security application that provides the security interface. The method of an embodiment comprises a second application engine coupled to the processor, wherein the second application engine executes a content application that provides the network interface.

The method of an embodiment comprises a core engine coupled to the processor, the core engine controlling dynamic provisioning of the plurality of applications and the content.

The core engine of an embodiment manages images received from a plurality devices of at least one of the security system and the LAN.

The images of an embodiment include video.

The processor of an embodiment is coupled to the WAN via a broadband coupling.

The processor of an embodiment is coupled to the WAN via a cellular coupling.

The plurality of interfaces of an embodiment provides interactivity with a plurality of devices via the plurality of interfaces.

A device of the plurality of devices of an embodiment is an Internet Protocol device.

A device of the plurality of devices of an embodiment is a camera.

A device of the plurality of devices of an embodiment is another touchscreen.

A device of the plurality of devices of an embodiment is a device controller that controls an attached device.

A device of the plurality of devices of an embodiment is a sensor.

Embodiments of the integrated security system include a method comprising: coupling a touchscreen including a processor to a local area network (LAN) and a security system at a first location; and displaying a plurality of interfaces to a user via the touchscreen, the plurality of interfaces displayed by a plurality of applications coupled to the processor, the plurality of interfaces including a security interface and a network interface, wherein the security interface provides the user with control of functions of the security system and access to data collected by the security system, wherein the network interface allows the user to transfer content to and from a remote network coupled to the LAN.

Embodiments of the integrated security system include a method comprising: coupling an input/output (I/O) device including a processor to a local area network (LAN) and a security system at a first location, wherein the security system includes a plurality of security system components that are proprietary to the security system; providing a security interface for control of functions of the security system, the security interface presented to a user via the I/O device, wherein a security application coupled to the processor generates the security interface; and providing a network interface for access to networked content of a remote network, the network interface presented to a user via the I/O device, wherein a content application coupled to the processor generates the network interface.

Aspects of the integrated security system and corresponding systems and methods described herein may be implemented as functionality programmed into any of a variety of circuitry, including programmable logic devices (PLDs), such as field programmable gate arrays (FPGAs), programmable array logic (PAL) devices, electrically programmable logic and memory devices and standard cell-based devices, as well as application specific integrated circuits (ASICs). Some other possibilities for implementing aspects of the integrated security system and corresponding systems and methods include: microcontrollers with memory (such as electronically erasable programmable read only memory (EEPROM)), embedded microprocessors, firmware, software, etc. Furthermore, aspects of the integrated security system and corresponding systems and methods may be embodied in microprocessors having software-based circuit emulation, discrete logic (sequential and combinatorial), custom devices, fuzzy (neural) logic, quantum devices, and hybrids of any of the above device types. Of course the underlying device technologies may be provided in a variety of component types, e.g., metal-oxide semiconductor field-effect transistor (MOSFET) technologies like complementary metal-oxide semiconductor (CMOS), bipolar technologies like emitter-coupled logic (ECL), polymer technologies (e.g., silicon-conjugated polymer and metal-conjugated polymer-metal structures), mixed analog and digital, etc.

It should be noted that any system, method, and/or other components disclosed herein may be described using computer aided design tools and expressed (or represented), as data and/or instructions embodied in various computer-readable media, in terms of their behavioral, register transfer, logic component, transistor, layout geometries, and/or other characteristics. Computer-readable media in which such formatted data and/or instructions may be embodied include, but are not limited to, non-volatile storage media in various forms (e.g., optical, magnetic or semiconductor storage media) and carrier waves that may be used to transfer such formatted data and/or instructions through wireless, optical, or wired signaling media or any combination thereof. Examples of transfers of such formatted data and/or instructions by carrier waves include, but are not limited to, transfers (uploads, downloads, e-mail, etc.) over the Internet and/or other computer networks via one or more data transfer protocols (e.g., HTTP, FTP, SMTP, etc.). When received within a computer system via one or more computer-readable media, such data and/or instruction-based expressions of the above described components may be processed by a processing entity (e.g., one or more processors) within the computer system in conjunction with execution of one or more other computer programs.

Unless the context clearly requires otherwise, throughout the description and the claims, the words "comprise," "comprising," and the like are to be construed in an inclusive sense as opposed to an exclusive or exhaustive sense; that is to say, in a sense of "including, but not limited to." Words using the singular or plural number also include the plural or singular number respectively. Additionally, the words "herein," "hereunder," "above," "below," and words of similar import, when used in this application, refer to this application as a whole and not to any particular portions of this application. When the word "or" is used in reference to a list of two or more items, that word covers all of the following interpretations of the word: any of the items in the list, all of the items in the list and any combination of the items in the list.

The above description of embodiments of the integrated security system and corresponding systems and methods is not intended to be exhaustive or to limit the systems and methods to the precise forms disclosed. While specific embodiments of, and examples for, the integrated security system and corresponding systems and methods are described herein for illustrative purposes, various equivalent modifications are possible within the scope of the systems and methods, as those skilled in the relevant art will recognize. The teachings of the integrated security system and corresponding systems and methods provided herein can be applied to other systems and methods, not only for the systems and methods described above.

The elements and acts of the various embodiments described above can be combined to provide further embodiments. These and other changes can be made to the integrated security system and corresponding systems and methods in light of the above detailed description.

In general, in the following claims, the terms used should not be construed to limit the integrated security system and corresponding systems and methods to the specific embodiments disclosed in the specification and the claims, but should be construed to include all systems that operate under the claims. Accordingly, the integrated security system and corresponding systems and methods is not limited by the disclosure, but instead the scope is to be determined entirely by the claims.

While certain aspects of the integrated security system and corresponding systems and methods are presented below in certain claim forms, the inventors contemplate the various aspects of the integrated security system and corresponding systems and methods in any number of claim forms. Accordingly, the inventors reserve the right to add additional claims after filing the application to pursue such additional claim forms for other aspects of the integrated security system and corresponding systems and methods.

What is claimed is:

1. A security system comprising:

a monitoring system that is configured to monitor a premise, the monitoring system including a sensor that is installed at the premise, the sensor being adapted to sense a status of the premise; and

a mobile device that is provided separately from the monitoring system by a company that is different than a company that provides the monitoring system, the mobile device including applications that, when run on the mobile device, perform operations comprising:

performing a synchronization to associate the mobile device with the monitoring system;

based on the synchronization, receiving by the mobile device one or more data communications descriptive of sensor events detected by the monitoring system at the premise;

displaying, on a display of the mobile device, a status interface area that includes status information related to the monitoring system based on the received one or more data communications;

displaying, on the display of the mobile device, a control interface area that enables a user to provide user input to control the monitoring system;

receiving user input defining a control operation for the monitoring system based on the control interface area; and

based on the received user input and the synchronization, sending one or more control communications that cause the monitoring system to perform the control operation defined by the received user input.

2. The security system of claim 1, wherein at least one of the applications is custom-built for the mobile device.

3. The security system of claim 1,

wherein the monitoring system is integrated with a monitoring system server that is located remote from the premise and that is configured to receive, over a network, data communications descriptive of sensor events detected by the one or more sensors included in the monitoring system; and

wherein performing the synchronization to associate the mobile device with the monitoring system comprises coordinating with the monitoring system server to synchronize with the monitoring system.

4. The security system of claim 3, wherein coordinating with the monitoring system server to synchronize with the monitoring system comprises synchronizing with the monitoring system server over the network, such that the mobile device exchanges, with the monitoring system server over the network, data communications descriptive of sensor events detected by the monitoring system at the premise.

5. The security system of claim 1, wherein receiving one or more data communications descriptive of sensor events detected by the monitoring system at the premise comprises receiving one or more data communications indicating that the monitoring system has detected an alarm event at the premise; and

wherein displaying a status interface area that includes status information related to the monitoring system comprises:

overriding a first application operating on the mobile device at a time of receipt of the one or more data communications, when the first application has been deteiniined to have a lower priority than the alarm event, and

displaying an alert that includes a description of the alarm event at the premise detected by the monitoring system, the alert replacing at least a portion of the first application content being displayed by the first application at a time of receipt of the one or more data communications.

6. The security system of claim 5, wherein the displaying the control interface area comprises displaying an input control that corresponds to a security operation that causes the monitoring system to perform an operation related to the alarm event; and

wherein the receiving user input comprises receiving, from a user, input corresponding to the security operation that causes the monitoring system to perform the operation related to the alarm event; and

wherein sending one or more control communications that cause the monitoring system to perform the control operation defined by the received user input comprises:

sending one or more control communications that cause the monitoring system to perform the alarm control operation defined by the received user input; and

resuming, on the mobile device, operation of the first application after receiving the user input activating the input control.

7. A method for protecting a premise, the premise protection method comprising the following operations:

performing, by a mobile device that is provided separately from a monitoring system that is configured to monitor a premise and includes a plurality of sensors that are installed at the premise and that are adapted to sense at least one status of the premise, a synchronization to associate the mobile device with the monitoring system that is configured to monitor the premise;

based on the synchronization, receiving by the mobile device one or more data communications descriptive of sensor events detected by the monitoring system at the premise;

displaying, on a display of the mobile device, a status interface area that includes status information related to the monitoring system based on the received one or more data communications;

displaying, on the display of the mobile device, a control interface area that enables a user to provide user input to control the monitoring system;

receiving by the mobile device a user input defining a control operation for the monitoring system based on the control interface area; and

based on the received user input and the synchronization, sending by the mobile device one or more control communications that cause the monitoring system to perform the control operation defined by the received user input.

8. The premise protection method of claim 7, wherein the mobile device includes at least one application that is custom-built for the mobile device and performs at least one of the operations.

9. The premise protection method of claim 7, wherein the monitoring system is integrated with a monitoring system server that is located remote from the premise and that is configured to receive, over a network, at least one data communication descriptive of sensor events detected by the plurality of sensors; and

wherein performing ling the synchronization to associate the mobile device with the monitoring system comprises coordinating with the monitoring system server to synchronize with the monitoring system.

10. The premise protection method of claim 9, wherein coordinating with the monitoring system server to synchronize with the monitoring system comprises synchronizing with the monitoring system server over the network, such that

the mobile device exchanges, with the monitoring system server over the network, the at least one data communication descriptive of sensor events detected by the monitoring system at the premise.

11. The premise protection method of claim **7**, wherein receiving one or more data communications descriptive of sensor events detected by the monitoring system at the premise comprises receiving at least one data communication indicating that the monitoring system has detected an alarm event at the premise;

wherein displaying a status interface area that includes status information related to the monitoring system comprises:

overriding a first application operating on the mobile device at a time of receipt of the data communication, when the first application has been determined to have a lower priority than the alarm event, and

displaying an alert that includes a description of the alarm event at the premise detected by the monitoring system, the alert replacing at least a portion of the first application content being displayed by the first application at a time of receipt of the data communication.

12. The premise protection method of claim **11**, wherein displaying a control interface area that enables a user to provide user input to control the monitoring system comprises displaying, concurrently with or after display of the alert, an input control that corresponds to a security operation that causes the monitoring system to perform an operation related to the alarm event;

wherein receiving user input defining a control operation for the monitoring system based on the control interface area comprises receiving user input activating the input control that corresponds to the security operation that causes the monitoring system to perform the operation related to the alarm event; and

wherein sending one or more control communications that cause the monitoring system to perform the control operation defined by the received user input comprises:

sending one or more control communications that cause the monitoring system to perform the security operation defined by the received user input; and

resuming, on the mobile device, operation of the first application after receiving the user input activating the input control.

13. A non-transitory computer-readable storage medium storing instructions that, when executed by one or more processors, cause the one or more processors to perform premise security operations comprising:

performing, by a mobile device that is provided separately from a monitoring system that is configured to monitor a premise and includes a sensor that is installed at the premise and that is configured to sense a status of the premise, a synchronization to associate the mobile device with the monitoring system that is configured to monitor the premise;

based on the synchronization, receiving one or more data communications descriptive of sensor events detected by the monitoring system at the premise;

displaying, on a display of the mobile device, a status interface area that includes status information related to the monitoring system based on the received one or more data communications;

displaying, on the display of the mobile device, a control interface area that enables a user to provide user input to control the monitoring system;

receiving user input defining a control operation for the monitoring system based on the control interface area; and

based on the received user input and the synchronization, sending one or more control communications that cause the monitoring system to perform the control operation defined by the received user input.

14. The non-transitory computer-readable storage medium of claim **13**, wherein at least a part of the instructions define at least one application that is custom-built for the mobile device and performs at least one of the operations.

15. The non-transitory computer-readable storage medium of claim **13**, wherein the monitoring system is integrated with a monitoring system server that is located remote from the premise and that is configured to receive, over a network, at least one data communication descriptive of sensor events detected by the one or more sensors included in the monitoring system; and

wherein performing the synchronization to associate the mobile device with the monitoring system that is configured to monitor the premise comprises coordinating with the monitoring system server to synchronize with the monitoring system.

16. The non-transitory computer-readable storage medium of claim **15**, wherein coordinating with the monitoring system server to synchronize with the monitoring system comprises synchronizing with the monitoring system server over the network, such that the mobile device exchanges, with the monitoring system server over the network, the at least one data communication descriptive of sensor events detected by the monitoring system at the premise.

17. The non-transitory computer-readable storage medium of claim **13**, wherein receiving one or more data communications descriptive of sensor events detected by the monitoring system at the premise comprises receiving at least one data communication indicating that the monitoring system has detected an alarm event at the premise; and

wherein displaying a status interface area that includes status information related to the monitoring system comprises:

overriding a first application operating on the mobile device at a time of receipt of the one or more data communications, when the first application has been determined to have a lower priority than the alarm event, and

displaying an alert that includes a description of the alarm event at the premise detected by the monitoring system, the alert replacing at least a portion of the first application content being displayed by the first application at a time of receipt of the one or more data communications.

18. The non-transitory computer-readable storage medium of claim **17**, wherein displaying a control interface area that enables a user to provide user input to control the monitoring system comprises displaying, concurrently with or after display of the alert, an input control that corresponds to a security operation that causes the monitoring system to perfoini an operation related to the alarm event;

wherein receiving user input defining a control operation for the monitoring system based on the control interface area comprises receiving user input activating the input control that corresponds to the security operation that causes the monitoring system to perform the operation related to the alarm event; and

wherein sending one or more control communications that cause the monitoring system to perform the control operation defined by the received user input comprises:

sending one or more control communications that cause the monitoring system to perform the security operation defined by the received user input; and

resuming, on the mobile device, operation of the first application after receiving the user input activating the input control.

* * * * *